Who Needs an Encryption Backdoor: Why Americans want Security over Privacy.

Robert E. Endeley
Adjunct Faculty, Dunwoody College of Technology
rendeley@dunwoody.edu

Abstract - **A qualitative analysis study that examined the views and opinions of non-technology professionals in the U.S. regarding government and law enforcement agencies' demand for legislation that will allow them to snoop on online private communications of smartphone users. Governments would prefer exclusive access to encryption technologies, called a backdoor, to use in accessing messages. Technology professionals have, however, argued against a backdoor; they claim a backdoor would not only be an infringement of their privacy but that hackers could also take advantage of it. In light of this security and privacy conflict between technology professionals and government's need to access messages in order to thwart potential terror attacks, this study presents the views and opinions of non-technology professionals in the U.S. who are the largest group of smartphone users, on the ensuing encryption debate. Using qualitative descriptive design methodology, a survey of 26 participants was conducted and data was analyzed using Braun and Clarke's six-step process of inductive thematic analysis. Results from this research study showed that non-technology professionals are willing to allow the government to infringe on their privacy if that will guarantee them security.**

Keywords: ***instant messaging, WhatsApp, end-to-end encryption, privacy, government***

I INTRODUCTION

Since smartphones became popular, many instant messaging (IM) services have been launched (Yeboah & Ewur, 2014). Some governments have become concerned about the ubiquity of IM services on mobile phones and their use of end-to-end encryption (E2EE) in safeguarding users' privacy, as it makes eavesdropping harder for them (Endeley, 2018; Michalas, 2017). E2EE ensures messages between communicating parties are secure, free from snooping, and hard to crack (Brantly, 2017). E2EE offers peace of mind to end users as it secures their data in transit and from third parties (Endeley, 2018). The service provider cannot access the messages, which can only be decrypted by the intended recipient (Michalas, 2017; "WhatsApp," 2017).

Governments would prefer special access to encryption technologies, called a backdoor, to use in accessing messages (Michalas, 2017). According to McCarthy (2016), a backdoor is an intentionally engineered gateway into the encryption system to provide an alternative means of accessing the encrypted content. An encryption backdoor may allow third parties to gain access to unencrypted data using certain keys (Abelson et al., 2015). The same backdoor used by an authorized third party such as a government agency authorized by court order may also be vulnerable to an unauthorized attacker who should not have access to the data (Abelson et al., 2015). Governments have emphasized they will only use the backdoor if there is a credible threat to national security (Brantly, 2017). In opposition to governments' proposals for a backdoor, Kern (2012) argued the promise of privacy guaranteed by modern encryption techniques, is, to a great extent, what has expounded the broad use of the internet. Kern further stated common online practices, such as online shopping, banking, and remote terminal services, would largely be impossible without the guarantee of the privacy and confidentiality provided by encryption.

According to Max (2016), governments and security agencies are wrong due to their unfounded belief that strong encryption that protects information on the internet, can at the same time be made weak in order to grant the government access to information.

The encryption and privacy debate heated up more recently following the indictment and conviction of President Donald Trump's former campaign manager, Paul Manafort: United States v. Manafort, District Court, District of Columbia (Novak, 2018). The federal prosecutors accused him amongst other things of witness tampering using the end-to-end encrypted messaging applications WhatsApp and Telegram (Novak, 2018). While E2EE ensures integrity, security, and privacy, it removes opportunities for government surveillance and the capacity to keep the nation secure by intercepting terrorist communications (Rastogi & Hendler, 2017).

According to McCarthy (2016), the Federal Bureau of Investigation (FBI) has been voicing concern that due to barriers such as strong encryption, government's security apparatus has been going dark in its attempt to monitor certain electronic communications and suspected terrorists. McCarthy revealed an increasing awareness of data-related privacy concerns in the aftermath of the Edward Snowden revelations made from 2013 onwards. These revelations purported to show the wide-reaching extent of bulk government surveillance by the U.S. and U.K. security agencies (McCarthy, 2016). McCarthy further stated the world's leading internet communication services providers such as Apple, Google, Facebook, WhatsApp, and Blackberry, have rushed to announce a renewed commitment to customer privacy. These companies all announced plans to implement E2EE on a default basis.

Law enforcement has been advocating for a backdoor into E2EE in IM services, thus undermining privacy and security (McCarthy, 2016). The New York County District Attorney, Cyrus Vance, in a written testimony to the U.S. Senate Judiciary Committee said Apple and Google smartphones should be configured to allow data on these devices to be accessed by law enforcement when it has judicial authorization to do so ("U.S. Department of Homeland Security," 201

Law enforcement agencies such as the FBI have argued to the U.S. Congress that the only way to compel smartphone manufacturers to comply with their request for a backdoor will be through legislation (Barr, 2016).

Much of the literature regarding the effects of E2EE on society has centered on the points of view of cryptographers and law enforcement agencies (Brantly, 2017). An in-depth review of the literature on this debate, however, showed no study had been done before in the U.S. to seek the opinions and views of non-technology professionals. Brantly, 2017 stated the former NSA and CIA Director, General (Ret.) Michael Hayden said, "we will only go as far as the American people allow us, but we will go all the way to that line" (p. 29). General (Ret.) Michael Hayden did not give any details following his statement on the view of the American people regarding encryption backdoors; he left it to anyone's imagination (Brantly, 2017). According to the "U.S. Census Bureau" (2016), technology professionals represent only 2.9 percent of the U.S. labor force.

Non- technology professionals, therefore, represent the largest segment of the labor force, and by inference the largest group of smartphone users ("U.S. Department of Labor," 2019; "U.S. Census Bureau," 2016). There are approximately 152 million working non-

technology professionals in the U.S. who will be impacted and are not aware ("U.S. Department of Labor", 2019; "U.S. Census Bureau", 2016). This study sought to understand the lengths at which nontechnology professionals would want the government to go regarding reading their private messages as a tradeoff for more security.

Studies have shown that non-technology professionals do not understand the impact of creating backdoors into encryption technologies (Sagers, Hosack, & Rowley, 2015; Wei et al., 2016

Non-technology professionals may not think of encryption very much, but it is fundamental to all our lives. Almost everything we do today on the internet uses a secret code, including internet banking, or logging on to Twitter or Facebook; encryption protects all such information. While E2EE protects users' IM from eavesdropping by third parties, full-disk encryption protects data such as photos, texts, emails, contacts, and bank account information from access by rogue individuals who may either steal your device or lay hands on a lost one (Herzberg & Leibowitz, 2016).

Vaziripour et al. (2018) asserted that non-technology professionals lack understanding of what an encrypted chat means and does to guarantee security. This study was, therefore, posited on the central question of whether non- technology professionals understood the impact of government-mandated backdoors on encrypted public messaging services. This study used a qualitative analysis methodology. A qualitative descriptive design was the selected design methodology for this study. A qualitative descriptive design study enabled accurate depictions of participants' views on the impact of government-mandated encryption backdoors (Dews-Farrar, 2018). Additionally, the researcher sought to augment the sparse number of scholarly qualitative descriptive studies concerning end-to- end encryption (E2EE), backdoors, and privacy.

The study intends to explore the following questions which serve as the primary focal points of this study:

- RQ1: Do non-technology professionals in the U.S. understand the impact of creating backdoors into end-to-end encrypted technologies?
- RQ2: What are the perspectives of non-technology professional users of IM applications regarding the argument security comes at a price, namely at the expense of privacy?
- RQ3: To what extent does the knowledge of encryption as a technology in safeguarding consumer privacy affect the use of the internet by non-technology professionals in the U.S.?

II RELATED WORK

Several authors have analyzed the intensifying debate on the proliferation of robust encryption technologies on mobile devices across the globe. In the FBI v. Apple case of 2016, the FBI wanted Apple to rewrite its operating system software (iOS), to disable encryption security features so the FBI could access the data (Elmer-Dewitt, 2016). A Pew survey showed in December 2015, the public sided with the FBI initially, with around 51% arguing Apple should help the FBI unlock the phone, 38% supporting Apple, and 11% not knowing enough about the dispute to form an opinion (Elmer-Dewitt, 2016). However, later polls in February 2016, with diverse methodologies, showed the public sided with Apple (Elmer-Dewitt, 2016). This demonstrated that by Apple making a strong public case in protecting the privacy of its users through the use of encryption, it also educated its user-base on their role in preserving user-privacy (Elmer- Dewitt, 2016). Apple's vigorous defense of its software shifted public opinion to its favor (Elmer-Dewitt, 2016)

According to a report published by the "U.S. Department of Homeland Security" (2015), the U.S. Senate held a hearing on whether recent technological changes have upset the balance between public safety and privacy. Law enforcement officials are becoming increasingly concerned that even after obtaining a warrant from a judge to search for evidence of a crime, they lack the technical means to do so ("U.S. Department of Homeland Security," 2015). This is due to companies increasingly choosing to encrypt devices in such a way the companies themselves are unable to unlock them, even when presented with a valid search warrant ("U.S. Department of Homeland Security," 2015). First, law enforcement agencies are reporting a decreasing ability to intercept real-time communications such as phone calls, text, email, and other types of data-in-transit ("U.S. Department of Homeland Security," 2015). Second, they relate a similar concern about their inability to execute search warrants on encrypted phones, laptops and other devices which contain data-at-rest ("U.S. Department of Homeland Security," 2015). Given this technological evolution, there is a potential impact on the fair and impartial application of the laws to everyone, as certain people are effectively placed outside the law ("U.S. Department of Homeland Security," 2015). The "U.S.

Department of Homeland Security" report concluded mandated technological weaknesses in encryption as proposed by some law enforcement agencies as a means of solving the problem of having exclusive access to these encrypted devices, are both futile and counterproductive. The report concluded Congress was open to reviewing ways to provide law enforcement with judicially-sanctioned access to these platforms without compromising overall security ("U.S. Department of Homeland Security," 2015).

In an article published by WIRED magazine in April 2018, former Microsoft Chief Software Architect and creator of Lotus Notes, Ray Ozzie, made a proposal at Columbia University on how to solve the impasse over secure backdoors between technology companies and law enforcement agencies (Levy, 2018). In his idea named CLEAR, Ozzie stated that his scheme would give law enforcement agencies access to encrypted data without significantly elevating the risks for billions of people who use encrypted devices such as mobile phones (Levy, 2018). Ozzie added the scheme works by technology companies such as Google or Apple generating two complementary keys: one called the vendor's public key, stored in every Android phone or tablet, and the other is called the vendor's private key (Levy, 2018). The private key is stored with Google and protected with the same tamper-proof care Google uses to certify its operating system updates (Levy, 2018). A combination of the private and public key pair can be used to encrypt and decrypt a secret PIN which each user's device automatically generates upon activation. It should be noted Ozzie's scheme attempts to solve the impasse with stored data (data at rest) and not the interception of real-time communications (data in transit) (Levy, 2018). According to Abelson et al. (2015), if law enforcement wants to assure itself access to real-time communications with backdoors, then intruders will also have an easier time getting access to real-time data.

Schneier et al., (2016) have pointed out countries such as the U.S., the U.K., and France seem very interested in mandating backdoors. The impetus to mandate backdoors in encryption products for the countries mentioned above is coming from law enforcement. Security researchers, according to Schneier et al. have, however, argued backdoors are impossible to implement securely and will result in reduced security for everyone. A practical limitation to mandating backdoors as a way of reducing crime is because encryption products come from different parts of the world (Schneier et al., 2016). Anyone attempting to evade encryption backdoors in the U.S., the U.K., or France has a wide variety of foreign encryption products to pick from which can encrypt hard drives, voice and text conversations, virtual private networks (VPN) links and everything else (Schneier et al., 2016). Schneier et al. identified 865 hardware or software encryption

products from 55 countries: 546 of these products, or two-thirds, were from outside the United States. Schneier et al. outlined that most common non-U.S. countries for encryption products were Germany, followed respectively by the United Kingdom, Canada, France, and Sweden. Germany and the Netherlands have publicly disavowed backdoors in all their encryption products.

III METHODOLOGY

The researcher conducted an Institutional Review Board (IRB) approved web and paper-based survey of non- technology professionals in the U.S. Since the study was designed for non-technology professionals, it was possible that not all of the participants will have access to the internet or own a computer. Hence, the need for a paper-based version of the survey. This study used a qualitative analysis methodology. The rationale for selecting a qualitative analysis for this research was based on the diagnosis of the purpose statement. Qualitative descriptive design method was the most appropriate for this research because it sought to gain insight into the views and opinions of non- technology professionals regarding their privacy on public communication platforms. Such an approach was especially useful for researchers wanting to know the "what" and "how" of events (Dews-Farrar, 2018).

A. Research Method and Design Appropriateness

The general population of the study were adult users of mobile phones located in the U.S. and running the latest version of end-to-end encrypted IM service, WhatsApp, on their mobile phones. The IM application WhatsApp was selected for this study because according to Sutikno, Handayani, Stiawan, Riyadi, and Subroto (2016), it is amongst the most favored IM applications endowed with E2EE. Jisha and Jebakumar (2014) stated WhatsApp is the fastest-growing IM application as most young people are moving away from Facebook. WhatsApp enjoys global favorability with a user base of over 1.5 billion subscribers. It is also the first application ever to implement E2EE to this scale (Rastogi & Hendler, 2017). From the target population, the researcher chose a research sample of 26 participants who met the criteria for participation.

B. Population, Sampling, and Data Collection Procedures and Rationale

This study posited non-technology professionals have a limited understanding of the consequences of a government- mandated backdoor into encryption technologies. The sample size of 26 for this study met the saturation limit in qualitative descriptive research as shown in similar research carried out by Dews-Farrar (2018) using the same design. The participants had to meet the following criteria: (a) Participants had to be owners of a mobile phone running the latest version of the WhatsApp application. (b) They had to be willing to participate in an online survey, or a face-to- face interview with the researcher. (c) They had to be non-technology professionals who at the time of this study did not have any experience working in technology or hold any diploma or certification in computer science, computer security or computer networking. (d) Participants had to be willing to give honest accounts of their views and opinions about privacy and national security.

C. Sampling

After obtaining IRB approval, the researcher initiated the participant recruitment process. Purposeful sampling, specifically the snowball sampling methodology, was used for the selection of the 26 participants. Purposeful sampling involves the selection of individuals who are qualified to provide in-depth information about the phenomenon being researched. Snowball sampling is a sub-category of purposeful sampling and has the advantage that after observing the initial participants, the researcher asks for assistance from the participants to help identify people with a similar trait (Creswell, 2015). Non-technology professionals like themselves who meet the requirements for the sample population (Creswell, 2015).

Snowball sampling is a non-probability sampling methodology. Rashidi, Vaniea, and Camp (2016) used snowball sampling in a study on privacy setting usage in WhatsApp application to recruit participants. The study by Rashidi et al. yielded relevant results which have contributed to the body of literature on how users manage privacy settings on IM applications. Snowball sampling generally consists of two steps:

1. The researcher identifies the potential participants in the population. Often, only a handful.
2. The researcher asks the identified participants to recruit other participants. The chain continues until the sample size is reached.

According to the Bureau of Labor Statistics of the "U.S. Department of Labor" (2017), States or jurisdictions with the highest location quotient for information technology experts are Virginia with 4.71, Maryland with 2.50, and the District of Columbia with 2.25. The location quotient is a way of quantifying how concentrated a particular industry or occupation is in a particular region or State, in reference to the entire nation. The States ranking with the lowest location quotient for information security experts are New Mexico, Missouri, and Colorado ranking 1.33, 1.37, and 1.41 respectively. The State of Minnesota falls in the middle of the rankings with 1.65 as its location quotient for information security experts. The average rankings in the distribution of technology professionals in Minnesota in relation to the rest of the country make it an ideal candidate for the target population of this study

D. Limitations

There were two limitations related to the data analysis of this study.

1. The sample population of this study was limited to a single state, Minnesota. The interpretation of results is affected by this limitation because it is not known if location quotient alone or the large population of healthcare workers in Minnesota introduced biases in the results.
2. Snowball sampling is a useful sampling methodology when it is not possible to use more traditional survey techniques. Snowball sampling technique, however, has its limitations. According to Sharma (2017), since snowball sampling does not select units for inclusion in the sample based on random selection, unlike the probability sampling technique, it is impossible to determine the possible sampling error and make generalizations from the sample to the population.

IV RESULTS

B. Pilot Study

A pilot study was carried out to establish the comprehensibility, validity, and reliability of the survey questions. The pilot study for this research consisted of five preliminary participants. The informed consent agreement was given to each participant, and the researcher obtained approval from all five participants. The pilot study revealed that the participants would be better served by defining key terms such as encryption, end-to-end encryption, and backdoors in the participant consent form before they got to the survey questions. Feedback from the pilot study was used to revise the final wording in the survey questions. The findings of this pilot study demonstrated the functionality of the survey instrument and the interest in the research by the target population. Thus, after adjustments to the survey from recommendations of the pilot study participants, the researcher concluded that the survey instrument was valid for this study's topic and served to answer the specific problems posited.

C. *Findings*

Forty-six participants in total responded to the survey between May 1, 2019, and May 10, 2019. Twenty of the respondents to the survey were eliminated during the data analysis phase because they did not meet the survey criteria. Twenty-six participants completed all the survey questions. Only responses of survey participants who met the survey criteria and completed all the questions are included in this article. The online web tool SurveyMonkey was used for preliminary analysis before respondent data were imported into NVivo data analysis software for full analysis.

D. *Demographics*

Out of the 26 participants who completed the survey, 12 (46.15%) were female, while 14 (53.85%) were male. Participants ranged in age from 25 – 70 years. The largest group of participants were between the ages of 45 - 54 years (46.15%), with the smallest between the ages 24 – 35 (7.69%) and 65 – 74 (7.69%). Figure 1 below shows the age distribution of participants. All 26 participants (100%) resided in the state of Minnesota, held no degree or certification in computer science, and their jobs did not include information technology-related activities. Table 1 below also displays a demographic summary of the participants.

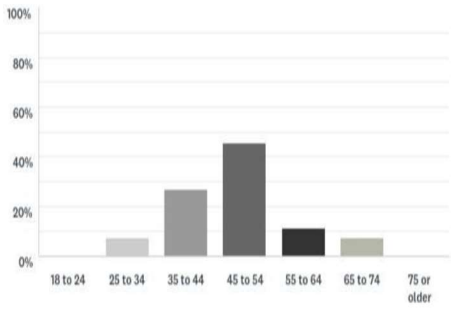

Fig 1. A bar chart showing the age distribution of participants

TABLE 1. DEMOGRAPHIC SUMMARY OF STUDY

Participant	Reside in Minnesota?	Hold computer certification?	Does your job include information technology related activities?	Age Group	Gende
P1	Yes	No	No	55 to 64	Male
P2	Yes	No	No	55 to 64	Femal
P3	Yes	No	No	35 to 44	Male
P4	Yes	No	No	35 to 44	Male
P5	Yes	No	No	45 to 54	Male
P6	Yes	No	No	45 to 54	Male
P7	Yes	No	No	45 to 54	Male
P8	Yes	No	No	45 to 54	Male
P9	Yes	No	No	45 to 54	Femal
P10	Yes	No	No	55 to 64	Male
P11	Yes	No	No	45 to 54	Male
P12	Yes	No	No	35 to 44	Male
P13	Yes	No	No	45 to 54	Male
P14	Yes	No	No	25 to 34	Femal
P15	Yes	No	No	45 to 54	Femal
P16	Yes	No	No	65 to 74	Femal
P17	Yes	No	No	45 to 54	Male
P18	Yes	No	No	35 to 44	Femal
P19	Yes	No	No	35 to 44	Femal
P20	Yes	No	No	45 to 54	Femal
P21	Yes	No	No	45 to 54	Femal
P22	Yes	No	No	65 to 74	Male
P23	Yes	No	No	35 to 44	Femal
P24	Yes	No	No	45 to 54	Male
P25	Yes	No	No	35 to 44	Femal
P26	Yes	No	No	25 to 34	Femal

Braun and Clarke's six-step inductive thematic data analysis approach was used to analyze the data. NVivo 12 Plus data analysis software for Windows was used in coding and analyzing the data for this study. Six themes emerged from the data analysis, namely: government and privacy, information, encryption, activities, communications, and social media. The themes were representative of participant- generated conceptualizations regarding the phenomenon encryption, backdoors, and privacy. Figure 2 below gives a visual representation of the six major themes generated from

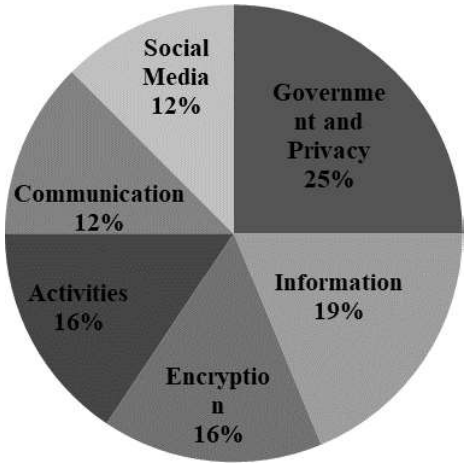

Fig. 2. A pie chart of the six themes generated from the study

the refinement of the initial codes through the process of eliminating redundancies and analysis (Creswell, 2015).

Some candidate themes were merged to form more coherent and meaningful themes; government and privacy themes were merged to form a single theme. The themes were validated as having a connection to the research questions and the overall research problem. The finalization of phase four led to phase five, which was to refine the themes and present them for data analysis.

Braun and Carke (2006) asserted that the researcher should not only be able to explain the relationship between the themes and the research questions but should additionally be prepared to construct an analysis of each theme. Each theme should portray the participants' collective perceptions of the phenomenon under research Braun and Clarke (2006). Figure 3 below shows the relationship between the research questions, codes, and themes.

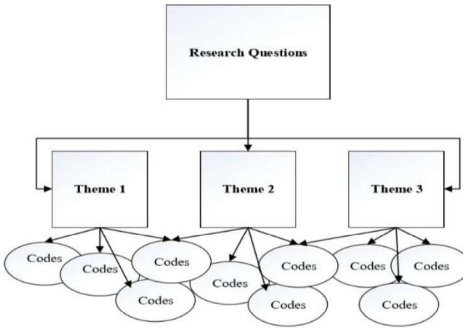

Fig. 3. The relationship between research questions, codes, and themes

E. *Findings and Interpretations*

Six themes emerged from the data analysis represent the survey participants' conceptualization regarding the phenomenon of the government exploring ways to implement encryption backdoors in popular messaging applications such as WhatsApp.

The themes provided closure for the three research questions that were the basis for this study. Data analysis of survey answers to RQ1 produced a single theme, government, and privacy.

1) Theme: Government and Privacy.

Twenty-three participants (88%) who coded for these themes showed a clear understanding of what an encryption backdoor meant and its impact on their privacy. This was significant to this research because it answered RQ1. Eleven of the participants (42%) were not opposed to the government adding a backdoor to read their private messages in order to keep them safe, especially if there is a credible threat against public safety. Further, these findings are even more significant because they validate the purpose of the research, which was to raise awareness for non- technology professional users of mobile devices on the benefits of encryption to privacy. When participants were asked at the end of the survey if this study had increased their knowledge or awareness of the benefits of end-to-end encryption to your privacy, 23 of the 26 of the participants (89%) responded that it had increased by a moderate amount, a lot, or a great deal. See table 3 below.

TABLE 2. HOW MUCH THE SURVEY IMPACTED PARTICIPANT KNOWLEDGE ON E2EE AND PRIVACY

Answer Choices	Responses	
A great deal	46.15%	12
A lot	23.08%	6
A moderate amount	19.23%	5
A little	11.54%	3
None at all	0.00%	0
Total		**26**

2) Theme: Information.

The sentiments expressed by 18 participants (69%) on this theme was neutral or mixed. Participants said that while they would like their private messages to remain private, they also do not mind the government stepping in to their private information in order to keep the country safe. This theme answered RQ2. Participants asserted through their responses that they are willing to allow the government to infringe on their privacy if that will guarantee them safety.

3) Theme: Activities.

Participants all expressed comfort in letting their security be of a higher priority than their privacy; thus, endorsing the government's intent to monitor electronic activities. This theme also answered RQ2.

4) Theme: Communications.

There were four participants (15%) who coded for this theme. Unlike participants who coded for the activities theme by expressing their comfort with government surveillance in exchange for security, communications participants were decisively against giving up their private communications in exchange for more security. This theme also answered RQ2.

5) Theme: Social Media.

Four participants (15%) expressed their views and opinions on how their knowledge of encryption will affect their use of social media applications such as WhatsApp.

This theme on social media was in response to RQ3, which asked participants to what extent the knowledge of encryption as a technology in safeguarding consumer privacy affect their use of the internet. Participants expressed more confidence in the use of the internet, knowing that encryption helps protect their communications.

6) Theme: Encryption.

Five participants (19%) coded for encryption. This theme was also in response to RQ3. Sixty percent of the participants who coded for this theme were concerned that terrorists could master encryption technology and use it to cause harm to society. In addressing RQ3, participants all agreed their knowledge of encryption would affect their use of the internet by increasing the confidence they have in the privacy of online communications. In addition to the two themes that emerged regarding RQ3, participants were given a layman's definition of encryption technology in the survey and asked if they were aware that popular websites such as Twitter, Facebook, or even their banking operations are all protected from hackers by encryption. Twenty-one participants (81%) answered yes, while five participants (19%) answered no. See figure 4 below.

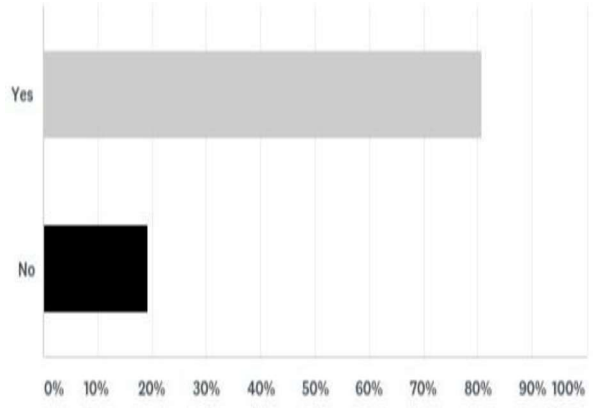

Fig. 4. A distribution graph showing participants knowledge on whether or not they knew encryption was used in protecting their data on popular websites such as Facebook and Twitter.

V. CONCLUSION

This study was relevant not only because it was aimed at filling some of the gaps in the literature regarding the opinions and views of non-technology professionals on the effects of end-to-end encryption (E2EE) on society but, it also confirmed and challenged previous studies on some of the privacy concerns expressed by U.S. mobile device users. Open-ended questions provided participants a means to best voice their experiences unrestricted by the influence of the researcher or past research findings (Creswell, 2015).

The results of this research study have confirmed some of the privacy concerns expressed by mobile device users, as mentioned by Rastogi and Handler (2017) and Elmer-Dewitt (2016). According to Elmer-Dewitt, following the standoff between Apple v.

FBI over access to the iPhone of the San Bernardino shooter, Americans, by a small margin (46% to 35%) support the government's right to access data in smartphones in order to protect the country against terror threats. This research study has also demonstrated that while concerned with their privacy, non-technology professionals are willing to allow the government to access their private messages if they have to do so in order to preserve national security.

Vaziripour et al. (2018) asserted the lack of understanding by non-technology professionals of what an encrypted chat means, as the reason for the none adoption of E2EE; this study proved the contrary. Eighty-one percent of participants who completed this research study said they were aware of what encryption was, and that is was used on most popular websites such as Twitter and Facebook to safeguard their private and sensitive information

Twenty-three participants (88%) showed a clear understanding of what an encryption backdoor meant and its impact on their privacy. A majority of participants (42%) were also not opposed to the government adding a backdoor to read their private messages in order to keep them safe, especially if there is a credible threat against public safety. Government has maintained that they will only use this method of access if there is a credible threat to public safety (Brantly, 2017).

Also, a majority participants (69%) said that while they would like their private messages to remain private, they also do not mind the government stepping in to their private information in order to keep the country safe.

A. Implications and Findings

The results of this study may also help educate the everyday user of the internet on the benefits of E2EE in their daily communications on mobile devices. Participants of this research study have said that it has significantly increased their knowledge of encryption. This creation of awareness and expectation of privacy guaranteed by strong encryption for the everyday user of the internet may also drive more technology companies to adopt E2EE, as was the case after the Edward Snowden leaks in 2013 (McCarthy, 2016). Another benefit this study may bring is, non-technology professionals may increase their adoption of using the internet for personal transactions such as paying bills, online banking, and money transfers once they are aware and understand the benefits of strong encryption on the internet. Participants of this study have expressed an increase in confidence in their privacy on the internet, knowing that encryption guarantees such privacy.

B. Strengths of this Study

There were four strengths in this research study. The first strength was that the researcher achieved data saturation through the participation of 26 working non- technology professionals who participated in the survey. The researcher's employment of structured and open-ended survey questions, a typical approach in qualitative inquiry, yielded detailed and insightful portrayals of the participants lived experiences and generated substantial data.

The second strength involved the use of a pilot study. According to Abdul, Othman, Mohamad, Lim, and Yusof (2017), survey questions could be strengthened by piloting the surveys. It can also help identify if there are flaws or limitations within the survey design that allow necessary modifications to the major study. (Abdul et al., 2017). The pilot study for this research established the comprehensibility, validity, and reliability of the survey questions. The survey questions were revisited to allow quality data and more in-depth responses from the participants.The third strength of this research study was the utilization of manual coding and subsequently, NVivo 12 Plus data analysis software. Prior to utilizing the NVivo 12 Plus qualitative data analysis program, each survey submission was read several times, portions of the text were highlighted in the Microsoft Word documents, and preliminary codes were identified in the right margin of the transcripts. Qualitative analysis depends to a good extent on the subjective interpretations of the researcher. Therefore, a combination of personal judgment and software was used to bring objectivity to the coding process. The utilization of NVivo data software increased the reliability and validity of the study.

The fourth strength was the large amount of qualitative data collected and the detailed descriptions of the participants' recounts and subsequent themes. The data allowed for thorough mining of codes during data analysis and subsequent validation with NVivo data analysis software. The research study was also able to capture participant's knowledge and awareness of E2EE at the beginning of the survey, and also evaluate if they have gained any additional knowledge during the course of the survey at the end.

C. Recommendations

This research study intends to augment the limited number of qualitative descriptive studies regarding the opinions and views of non-technology professionals on the benefits of E2EE on society. The results from this study have revealed insightful accounts of 26 non-technology professionals in the U.S. on E2EE, backdoors, and privacy. Based on the results of this research study the following are recommendations for future research:

1) Extend the research sample area beyond the state of Minnesota to other states. The State of Minnesota falls in the middle of the rankings for the location quotient for information security experts ("U.S. Department of Labor," 2017). Therefore, it is recommended that states with the highest location quotient for information security experts such as Virginia and Maryland, as well as states with the lowest location quotient for information security experts such as New Mexico, Missouri, and Colorado, be sampled.
2) Perform a quantitative study of non-technology professionals with a random sample of participants distributed across the US. This would eliminate some of the inherent weaknesses expressed in the limitations of this research study on the snowball sampling methodology.
3) Include the influence of gender, age, ethnicity, or level of education on participants' views on the government's demand for a backdoor into encryption systems could be an interesting area of research. Similar studies carried out in Iran by Vaziripour et al. (2018) on the Telegram IM application showed that skewed demographics might have influenced the results of the research.
4) Expand this research study internationally, into other countries with less cellphone penetration than the U.S. As mentioned by Schneier et al. (2016), encryption is now a global phenomenon. Laws in the U.S. mandating backdoors into encryption systems will primarily affect only U.S. users of encryption products made in the U.S. (Schneier et al., 2016). Smartphone users in other countries rely on other products. The literature review conducted for this research study found out countries such as Germany, United Kingdom, Canada, France, and Sweden also produce a lot of encryption products (Schneier et al., 2016). Researching the perspectives of people of other countries on this topic would certainly add value to the body of literature in cybersecurity.

REFERENCES

Abelson, H., Anderson, R., Bellovin, S. M., Benalo, J., Blaze, M., Diffie, W.,… Weitzner, D. J. (2015). Keys under doormats: Mandating insecurity by requiring government access to all data and communications. *Computer Science and Artificial Intelligence Laboratory Technical Report*, MIT-CSAIL-TR-2015-026. doi: http://hdl.handle.net/1721.1/97690

Abdul, M. M, Othman, M., Mohamad, S. F., Lim, S. A., & Yusof, A. (2017). Piloting for interviews in qualitative research: Operationalization and Lessons Learnt. International Journal of Academic Research in Business and Social Sciences. 7(*4*). doi:10.6007/IJARBSS/v7-i4/2916

Barr, A. C. (2016). Guardians of Your Galaxy S7: Encryption backdoors and the first amendment. *Minn.L. Rev.*, *101*, 301-383. Retrieved from http://www.minnesotalawreview.org/wp-content/uploads/2016/11/Barr.pdf

Brantly, A. F. (2017, August). Banning encryption to stop terrorists: A worse than futile exercise. *Combating Terrorism Center at West Point, CTCSENTINEL, 10*(7), 29-35. Retrieved from https://ctc.usma.edu/banning-encryption- to-stop-terrorists-a-worse-than-futile-exercise/

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101. http://dx.doi.org/10.1191/1478088706qp063oa

Creswell, J. W. (2015). *Educational research: planning, conducting, and evaluating quantitative and qualitative research*. Upper Saddle River, NJ: Pearson Education, Inc.

Dews-Farrar, V. (2018). *Students' reflections and experiences in online learning: A qualitative descriptive inquiry of persistence* (Order No. 10809354). Available from ProQuest Dissertations & Theses Global. (2036952458). Retrieved from https://search.proquest.com/docview/2036952458

Elmer-Dewitt, P. (2016). Apple vs. FBI: What the polls are saying. *Fortune*. Retrieved from http://fortune.com/2016/02/23/apple-fbi-poll-pew

Endeley, R. E. (2018). End-to-end encryption in messaging services and national security - case of WhatsApp messenger. *Journal of Information Security, 9*(1), 95-99. https://doi.org/10.4236/jis.2018.91008

Fink, A. (2018). *How to conduct surveys*. A step-by-step guide. Thousand Oaks, CA: Sage Publications, Inc.

Herzberg, A., & Leibowitz, H. (2016). Can Johnny finally encrypt? Evaluating E2E-encryption in popular im applications. doi:10.1145/3046055.3046059.

Hilal, A. H., & Alabri, S. S. (2013). Using NVIVO for data analysis in qualitative research. *International Interdisciplinary Journal of Education, 2*(2), 181–186.

Jisha, K., & Jebakumar. (2014). A trend setter in mobile communication among Chennai youth. *IOSR Journal of Humanities and Social Science (IOSR-JHSS), 19*(9), 01-06. doi: 10.9790/0837-19970106

Jones, J., Turunen, H., & Snelgrove, S. (2016). Theme development in qualitative content analysis and thematic analysis. *Journal of Nursing Education and Practice, 6*(5), 100.

Kern, D. (2012). Understanding and implementing encryption backdoors. Retrieved from http://cse.ucdenver.edu/~dkern/CSC7002/paper.pdf

Levy, S. (2018, April). Cracking the crypto war. *WIRED*. Retrieved from https://www.wired.com/story/crypto-war-clear-encryption/ Lewis, J., Zheng, D., & Carter, W. (2017, February). The effect of encryption on lawful access to communications and data. *A report of the CSIS Technology Policy Program.*Washington, DC: Center for strategic and international studies

Max, Steven Patterson. (2016, April). WhatsApp copies apple's strong encryption defense. *Network World*, Southborough. Retrieved from https://search.proquest.com/docview/1779534877?accountid =44888

McCarthy, H. J. (2016). Decoding the encryption debate: Why legislating to restrict strong encryption will not resolve the "going dark" problem. *Journal of Internet Law. 20*(3). Retrieved from https://www.slideshare.net/HughJMcCarthy/decoding-the-encryption-debate-hugh-j-mccarthy-september-2016222905691pdf

Michalas, A. (2017). How WhatsApp encryption works - and why there shouldn't be a backdoor. The Conversation. Retrieved from https://theconversation.com/how-whatsapp-encryption- works-and-why-there-shouldnt-be-a-backdoor-75266

Novak, M. (2018). Paul Manafort learns that encrypting messages doesn't matter if the feds have a warrant to search your iCloud account. Retrieved from https://gizmodo.com/paul-manafort-learns-that-encrypting- messages-doesnt-ma-1826561511

Rashidi, Y., Vaniea, K., & Camp, J. (2016). Understanding Saudis' privacy concerns when using WhatsApp. doi:10.14722/usec.2016.23022.

Rastogi, N., & Hendler, J. (2017, June). WhatsApp security and role of metadata in preserving privacy. *Paper presented at the European Conference on Cyber Warfare and Security 269-XVI.* Dublin, Ireland.

Sagers, G., Hosack, B., & Rowley, R. (2015). *Where's the security in WiFi? An argument for industry awareness.* 48th Hawaii International Conference on System Sciences. IEEE Computer Society. Washington, DC, USA

Salkind, N. J. (2012). *Exploring research.* Upper Saddle River, NJ: Pearson Education, Inc.

Schneier, B., Seidel, K., & Vijayakumar, S. (2016). A worldwide survey of encryption products. *Berkman Center Research Publication 2016-2*. http://dx.doi.org/10.2139/ssrn.2731160

Shah, R. (2016). Law enforcement and data privacy: A forward-looking approach. *The Yale Law Journal, 125*(2), 326-559. Retrieved from http://digitalcommons.law.yale.edu/ylj/vol125/iss2/5

Sharma, Gaganpreet. (2017). Pros and cons of different sampling techniques. *International Journal of Applied Research 2017, 3*(7), 749-752.

SurveyMonkey Inc. (2019). Retrieved from www.surveymonkey.com. San Mateo, California, USA

Sutikno, T., Handayani, L., Stiawan, D., Riyadi, M. A., & Subroto, I. M. I. (2016). WhatsApp, Viber and Telegram which is best for instant messaging? *International Journal of Electrical and Computer Engineering, 6*(3), 909-914. doi: 10.11591/ijece.v6i3.10271

U.S. Census Bureau. (2015, June). Millennials Outnumber Baby Boomers and Are Far More Diverse, Census Bureau Reports. Release number CB15-113. Retrieved from https://www.census.gov/newsroom/press-releases/2015/cb15-113.html

U.S. Census Bureau. (2016, August). Number of IT workers has increased tenfold since 1970, census bureau reports. Retrieved from https://www.census.gov/newsroom/press- releases/2016/cb16-139.html

U.S. Department of Homeland Security. (2015, July). Going Dark: Encryption, Technology and the Balance between Public Safety and Privacy. *Senate Committee on the Judiciary.* Homeland Security Digital Library

U.S. Department of Labor. (2017). Bureau of Labor Statistics. Occupational employment statistics. Retrieved from https://www.bls.gov/oes/current/occ_state_lq_chart/occ_state_lq_chart.htm#

U.S. Department of Labor. (2019). Bureau of Labor Statistics. Labor force statistics from the current population survey. Retrieved from https://www.bls.gov/cps/cpsaat11b.htm

Vaziripour, E., Wu, J., Farahbakhsh, R., Seamons, K., O'Neill, M., & Zappala, D. (2018). *A survey of the privacy preferences and practices of iranian users of telegram*. Workshop on Usable Security (USEC). San Diego, CA. https://dx.doi.org/10.14722/usec.2018.23033

Wei, B., Doowon, K., Moses N., Yichen Q., Patrick G., & Michelle L. (2016). *An inconvenient trust: User attitudes toward security and usability tradeoffs for key-directory encryption systems*. Twelfth Symposium on Usable Privacy and Security. Denver, CO

WhatsApp (2017, December). WhatsApp encryption overview. *Technical white paper.* Retrievedfrom https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

Yeboah, J., & Ewur, G. (2014). the impact of WhatsApp messenger usage on students performance in tertiary institutions in Ghana. *Journal of Education and Practice, 5*(6), 157-164. Retrieved from https://www.iiste.org/Journals/index.php/JEP/article/view/11241

