2021

Mobile Forensics: The Perception of Privacy

Charlsea Young
Walden University

Walden University

College of Social and Behavioral Sciences

This is to certify that the doctoral dissertation by

Charlesa Young

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Joseph Pascarella, Committee Chairperson,
Criminal Justice Faculty

Dr. Marisa Bryant, Committee Member,
Criminal Justice Faculty

Dr. Joseph McMillan, University Reviewer,
Criminal Justice Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2021

Abstract

Mobile Forensics: The Perception of Privacy

by

Charlesa Young

MA, University of Maryland University College, 2015

BS, Alabama State University, 2011

Project Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Criminal Justice

Walden University

August 2021

Abstract

Technology companies like Apple pride themselves on protecting its consumers' data, which they express within their mission statement and by also encrypting their mobile devices. This encryption stalled an investigation conducted by the Federal Bureau of Investigation in 2016, resulting in them taking Apple to court. There has been a lack of information about mobile forensic examiners perceptions on issue they face in the mobile forensic field. The purpose of this research study was to address the perceptions mobile forensic examiners experience when dealing with encryption, privacy, and national security concerns. This qualitative phenomenological study included interviews with 10 mobile forensic examiners (two female and eight male) with at least 1 year of experience on key issues in the mobile forensic field. Results from this study, identified that mobile forensic examiners wanted to work with technology companies on encryption issues, however they did not have a solution on how to begin. Findings from this study can be used to move forward the conversation between the technology companies and mobile forensic examiners, in order to come to an understanding with each other, with a comprise everyone can live with. Future research can gather information on how the technology companies perceive the privacy and encryption concerns, resulting in positive social change.

Mobile Forensics: The Perception of Privacy

by

Charlesa Young

MA, University of Maryland University College, 2015

BS, Alabama State University, 2011

Project Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Criminal Justice

Walden University

August 2021

Dedication

I would like to take this opportunity to thank my family for helping me throughout this rewarding process. To my mother Celean and father Anthony, thank you both for always believing in me and allowing me to live out my wildest dreams. I want to thank my little sister Aaliyah, for always giving me a reason to strive for the moon, as setting a great example has and will always be my goal. My brother Anthony Jr. for never missing an opportunity to tell me how proud of me you are. To all my friends and family that have been with me throughout this entire process, motivating me to keep going. Finally, to my big sister/role model Charlena, because you I have accomplished a goal I never could have imaged. Thank you for pushing me to not only start this journey, but to continue and finish it as well.

Acknowledgement

I would like to acknowledge my entire committee Chair Dr. Joseph Pascarella, Committee Member Dr. Marisa Bryant and University Research Review Dr. Joseph McMillan on helping me throughout this entire process and providing me with valuable feedback. Thank you all for your support on this journey.

Table of Contents

List of Tables vi

List of Figures vii

Chapter 1: Introduction to the Study 1

Introduction 1

Background 1

Problem Statement 2

Purpose 3

Research Questions 4

Framework 4

Nature of the Study 5

Definitions 5

Assumptions 6

Scope and Delimitations 7

Limitations 7

Significance 8

Summary 8

Chapter 2: Literature Review 10

Introduction 10

Interpretivism 11

Mobile Phones 11

Privacy 12

Legal Laws 14
Fourth Amendment 14
FBI v. Apple 19
Digital Forensics 21
Cellebrite 22
GrayKey 23
Digital Evidence 24
Encryption 26
Mobile Forensics 26
Seizure/Preservation 27
Acquisition 28
Examination/Analysis 30
Reporting 33
Summary 33
Chapter 3: Methodology 35
Introduction 35
Research Design 35
Role of the Researcher 35
Research Questions 36
Sampling of Participants 36
Data Collection 37
Reliability and Validity 39

Data Analysis 39
Ethical Protections 41
Summary 42
Chapter 4: Results 43
Introduction 43
Study Overview 43
Personal and Organizational Influences 44
Data Analysis and Collection Procedures 45
Interview Data 50
Participant 1 50
Participant 2 50
Participant 3 51
Participant 4 52
Participant 5 52
Participant 6 53
Participant 7 55
Participant 8 56
Participant 9 56
Participant 10 58
Themes by Interview Question 59
Interview Question 1 59
Interview Question 2 59

Interview Question 3 59
Interview Question 4 60
Interview Question 5 60
Interview Question 6 61
Interview Question 7 61
Interview Question 8 61
Interview Question 9 62
Interview Question 10 62
Interview Question 11 62
Themes by Research Question 63
RQ1 63
RQ2 64
Summary 64
Chapter 5: Conclusions and Recommendations 66
Introduction 66
Results Summary 66
Findings 67
Limitations 68
Social Change 68
Recommendations 69
Personal Reflections 69
Conclusion 70

References 71

Appendix A: Letter of Invitation 79

Appendix B: Interview Questions 80

List of Tables

Table 1. Participants Demographics 48

List of Figures

Figure 1. GrayKey Customer Research 23

Figure 2. Mobile Forensic Investigation Process..... 27

Figure 3. Acquistion Phase 29

Figure 4. GAFAM: Women Still Underrepresented in Tech 49

Chapter 1: Introduction to the Study

Introduction

The purpose of this qualitative research study was to understand the barriers criminal investigators face when conducting mobile forensics investigations. While considering such barriers, security and privacy were also researched in terms of national security and mobile forensics. Cultural differences between law enforcement and tech companies were acknowledged when considering national security and privacy. One-on-one interviews with forensic examiners and criminal investigators as well as individuals from the private sector with different backgrounds helped fill a gap in research involving individuals' perceptions concerning mobile forensics security and privacy. This helped in terms of addressing the importance of law enforcement perceptions regarding how they feel about barriers when mobile forensics meets national security and privacy at the same time.

Background

In 2016, The Federal Bureau of Investigation (FBI) responded to an active shooter incident in San Bernardino, CA. Upon responding to the incident and the shooter being fatally shot, agents wanted to gain access to the suspect iPhone. The FBI attempted to work with Apple to gain access via a backdoor, however Apple refused to help, stating privacy and security concerns if they created a backdoor to the device. This resulted in the FBI taking Apple to court, attempting to force them to work with them, by citing national security concerns. During the Apple v. FBI case, it was clear that there was a lack of standards pertaining to national security, privacy, and mobile forensics. The court

did not get a chance to rule on whether Apple needed to create a back door for the FBI to access the device, as the FBI decided to drop the case prematurely and find alternative routes to get the information they needed. There is information concerning why mobile forensics is a method for law enforcement conducting investigations; however, there is a lack of information concerning costs of mobile forensics when considering privacy and national security. This is an issue that will get worse until the matter is addressed.

Problem Statement

The criminal justice system has an enduring issue that has never been properly resolved. That issue involves the amount of privacy citizens expect when it comes to their media equipment and criminal investigations conducted by law enforcement. According to Levy (2017), the Federal Bureau of Investigation (FBI) devalues privacy rights by coveting Apple's security features to get into possible suspect iPhones. In 2016, an active shooter incident in San Bernardino, California demonstrated the amount of pressure and limits preventing law enforcement agencies from getting access to individuals' personal devices in order to obtain what may be incriminating evidence. Mobile devices can hold a plethora of information on them to include calls logs, pictures, passwords, GPS data, system files and deleted data (Gillware, n.d.).

According to the Interagency Security Committee (ISC, 2015), there were over 160 active shooter incidents with 1,043 casualties between 2000 and 2013. Law enforcement serves as a form of protection to the public from those who have committed horrendous acts of crime. Companies were formerly against encryption security measures in their products; however, this has drastically changed over time, and now they are

refusing to not encrypt their products, causing concern for law enforcement agencies (Hosein, 2017). There is a lot of discussion on the topic; however, there is a lack of information regarding how individuals outside the tech and law enforcement field feel about the issue and how they perceive it. According to Makin and Morczek (2015), telecommunication providers can supply investigators with voice mail, call logs, and codes for accessing data contained on subscriber identity modules (SIM); however, those same companies can make it extremely difficult to trace communication because of legal processes that are potentially required. There is a lack of guidance throughout the criminal justice field in terms of what procedures and processes need to take place for investigators to conduct their investigations, especially when concerning mobile forensics. According to Cisco (2016), there were 11.6 billion mobile-connected devices in the year 2020. This study will fill the gap of lack of communication and understanding mobile forensic examiners and technology companies currently have amongst each other. Expanding and contributing to the body of knowledge needed to address this problem by addressing what the public, tech companies, and government agencies can do to discuss the issue with a possible compromise between security and privacy.

Purpose

The purpose of this qualitative research study was to understand barriers criminal investigators face when conducting mobile forensics investigations. While considering such barriers, security and privacy were also researched in terms of national security and mobile forensics. Focusing mainly on mobile forensics investigations, culture differences between law enforcement and the public were acknowledged when considering national

security and privacy. One-on-one interviews with forensic examiners and criminal investigators as well as individuals from the private sector with different backgrounds helped fill gaps in research where individuals' perceptions concerning mobile forensics security and privacy had been vague. This helped in terms of acknowledging the importance of forensic examiners' perceptions regarding how they felt about barriers involving mobile forensics meeting national security and privacy issues at the same time.

Research Questions

RQ1: What is the impact of encryption on mobile forensic investigations?

RQ2: When considering national security, what are the perceptions of mobile forensic investigators concerning privacy rights?

Framework

The theoretical approach for this research study was Husserl's phenomenology theory in which he focused on ideas. The phenomenology theory has been used throughout multiple studies involving individuals' perceptions regarding incidents they have lived to experience. As forensic examiners have lived numerous experiences where they have dealt with encryption on mobile devices and had difficulty cracking the encryption, using this theory will help in terms of addressing their thoughts on the issue.

Husserl's phenomenology theory involves the perceptions of individuals. According to Smith (2016), phenomenology involves developing a descriptive or analytic psychology in that it describes and analyzes types of subjective mental activity or experiences. Blasdel (2010) said the purpose of using the phenomenological approach is to identify common themes.

. The phenomenology theory involves researchers including and reflecting on their own experiences in ways that elicit deeper and more profound participant responses (Miner-Romanoff, 2012). As a researcher, reflecting on personal experiences can in many ways be a potential weakness of this theory, as it may sway participants' responses based of how questions are presented. Alawadhi (2019) said "researchers must aim to remove theory from the description of the phenomenon, or to bracket perceived notions and prejudices" (p. 79).

Nature of the Study

The nature of this research study was qualitative. Use of the qualitative approach allowed for perceptions of mobile forensic examiners to be coded and analyzed for potential themes. These themes were used to understand if there were potential patterns that existed when considering mobile forensics, privacy, and national security. Using an inductive approach, I analyzed themes from participants' interviews to gain a generalized understanding. In order to understand barriers that mobile forensic examiners face when trying to conduct criminal investigations, Husserl's phenomenology theory was applied. These barriers were discussed with forensic examiners, which may contrast with how tech companies may feel about the same issues.

Definitions

Acquisition: The process of making a forensic image from computer media such as a hard drive, thumb drive, CD-ROM, removable hard drives, servers, and other media that stores electronic data including gaming consoles and other devices (Universal Data Acquisition, n.d).

Digital Forensics: The process of preservation, identification, extraction, and documentation of computer evidence which can be used in a court of law.

Encryption: The process of changing plain text into random characters that only can only be decoded with the right passcodes.

Federal Forensic Examiner: Examiners who work at the federal government level, instead of state and local levels.

Imaging: Copying a physical storage device for conducting investigations and gathering evidence (Griffin, 2018).

Mobile Forensics: A branch of digital forensics which involves acquisition and the analysis of mobile devices to recover digital evidence of investigative interest (Dcng, 2015).

Mobile Forensic Examiner: A forensic examiner who tends to specialize in mobile devices such as smartphones.

Assumptions

This study assumed that individuals participating in this study felt very strong about mobile forensics being an important field in digital forensics, especially when concerning criminal investigations, therefor their perceptions on what effects the field is important too. As participants use mobile forensics regularly to solve criminal investigations, they are not the decision makers when it comes to the scope of information they are allowed to collect or not. However, it was assumed that they were in position to best help decision makers understand the importance of mobile forensics and why sometimes individuals' privacy may have been violated.

As forensic examiners often have some discretion when it involves mobile forensic investigations, it can be difficult to assume whether or not information retrieved in this investigation were rightly retrieved or viewed. This is important to acknowledge as privacy is one of the focal issues within this research study.

Scope and Delimitations

The study involved using interviews to understand participants' perceptions regarding privacy and mobile forensics. Data was collected form a small participant group who were available to speak via video chat and had at least 1 year of experience with mobile forensics. As mobile forensics is a very specialized field, participants were expected to be technical inclined, as I was not planning to explain the field of mobile forensics. In order to address the potential of transferability, themes were compared to research concerning computer forensic encryption issues. There was a lack of scholarly research available to draw from regarding mobile forensic examiners perceptions on encryption, privacy, and national security. Detailed emails were sent to all participants who agreed to interviews, therefor ensuring every participant understood what they were agreeing to.

Limitations

Only certain mobile forensic examiners who had at least a year of experience were interviewed, as it would be impractical to speak with mobile forensic examiners who lack real experience in the field. This also created some limitations and bias because individuals with less than a year of experience could still potentially have provided valuable information. These limitations and biases were addressed by having a mix of

individuals participate who were randomly selected via social media and had different backgrounds in the field.

Significance

This study helped fill in gaps regarding many issues law enforcement and mobile forensic examiners face when dealing with national security and privacy. Most federal law enforcement depend on evidence found on individuals' personal devices when conducting investigations. With the current issue of security and privacy overlapping one another, there must be clear standards in order to protect everyone involved. Focusing on barriers that come along with mobile forensics and privacy, this study will afford policy makers the opportunity to see, understand, and address these barriers that law enforcement investigators feel could hinder them from conducting mobile forensic investigations and still maintain privacy for individuals. This research study contributed to discussions regarding technology companies and law enforcement concerning building back doors to mobile devices, especially when national security may be of concern.

Summary

In this chapter, I discussed the purpose and background of this study, while also acknowledging a gap in research concerning digital forensics. While addressing this gap, I also address the limitations that the study may face. The assumption that mobile forensics was one of the most important aspects of criminal investigation was also discussed. Definitions of terminology used throughout research were listed In Chapter 2, I address mobile forensics and the process of conducting examinations along with previous laws that have been established concerning privacy and electronic devices. I will

also discuss relevant research studies concerning issues technology companies and forensic examiners face dealing with encryption methods.

Chapter 2: Literature Review

Introduction

This study will provide a deeper understanding of participants' perceptions based on previous issues concerning mobile forensics in criminal investigations. There is a lack of research available regarding mobile forensics and encryption when it comes to investigations and how encryption plays a major role in examiners being able to conduct their examinations in a thorough and timely manner. Information was compiled from sources such as legal documents, news articles, and interviews with professionals in the field.

These sources focused on experiences individuals had, or situations that happened. According to Moustakas (1994), "phenomenology is focused less on the interpretations of the researcher and more on a description of the experiences of participants" (p. 165). Using the phenomenology theory, I was able to gain understanding of the concerns forensic examiners have when attempting to conduct their investigations in a timely manner. Thanh and Thanh (2015) said researchers who use the interpretivist paradigm and qualitative methods often seek experiences, understandings, and perceptions of individuals for their data to uncover reality rather than rely on numbers or statistics.

While the purpose of this study is to gain a better understanding of why privacy and mobile forensics can sometimes cause concerns for individuals, this study also involves different aspects of mobile forensics and privacy rights. Along with researching mobile forensics, this study also addressed different aspects of forensics such as digital

evidence. Using the Fourth Amendment and notable Supreme Court cases, this chapter includes information regarding how mobile forensics is becoming a gray area that will eventually need to be addressed as the field is continues to grow and expand.

Criminal investigations are constantly being subverted by digital evidence and anything digital can store evidence within it. This has created an unprecedented issue in the criminal justice and law enforcement fields, especially when it relates to mobile and smartphones. As these devices continue to advance, individuals' privacy continues to be discussed.

Interpretivism

When considering research on the perception of mobile forensics examiners, utilizing an interpretivist philosophy would be ideal. Dudovskiy (n.d.) said interpretivism is "associated with the philosophical position of idealism, and is used to group together diverse approaches, including phenomenology; an approach that reject the objectivist view that meaning resides within the world independently of consciousness" (Dudovskiy, n.d, as cited in Collins, 2010). When discussing individuals' privacy, it can often be a very subjective matter, and views can often be based off individuals' perceptions of situations.

Mobile Phones

Mobile phones, smartphones, and PDAs have increased among individuals throughout the world. According to Tamma et al. (2018), "the number of mobile phones users in the world was expected to surpass 5 billion in 2019" (p. 8). Mobile phones are used during individuals' everyday lives for paying bills, taking pictures, and calendar

appointments. e This has led to individual personal lives being documented within their phones either internally or externally via social media sites.

The Samsung Galaxy and iPhone are two of the most popular smartphone devices available in the mobile phone market. These devices come with unique platforms that usually help users determine which one best fit their needs. Android operating systems occupy over 80% of mobile devices markets based on 2017 statistics, with iOS second (Mikhaylov, 2017). This could be because of Android's user-friendly interface that allows the user to control everything their phone does, unlike its competitor Apple iOS.

Freedom of control in terms of Android and Apple devices tend to play a notable role when it comes to security and privacy. Security and privacy are two factors that lead to debates between users of devices and individuals who manufacture the devices along with forensic examiners in the digital forensic field. Data can be stored on mobile devices that can become vulnerable to hacking (Au et al., 2017). Mobile devices are becoming smarter, with every newly updated release model boasting better security and privacy encryption.

Privacy

Individuals tend to define privacy differently based on what they consider private or not. Protecting data on smartphones and privacy has been an important topic for many years. While technology companies pride themselves on protecting their consumers' data from law enforcement, this has been debated and questioned. Newman (2012) said law enforcement has continued to decry that smartphone encryption methods hinder their investigations, which can potentially lead to national security concerns.

Smartphones now have a multitude of protection layers to disrupt any unwarranted access to devices without proper passcodes. While iOS has infrastructure in place for hierarchical encryption protection, much of it is unused and operation systems do not extend encryption protections as far as it could (Newman, 2021). According to Newman (2021),

> When an iPhone has been off and boots up, all the data is in a state Apple calls complete protection. The user must unlock the device before anything else can really happen, and the device's privacy protections are very high. You could still be forced to unlock your phone, of course, but existing forensic tools would have a difficult time pulling any readable data off it. Once you have unlocked your phone that first time after reboot, though, a lot of data moves into a different mode—Apple calls it Protected Until First User Authentication, but researchers often simply call it "After First Unlock. (para. 7)

There is a concern because individuals do not tend to reboot their devices very often, which means that most devices will be in a state after first unlock more often than completely protected.

Everything done on a smartphone can lead to some type of privacy concern. For example, taking a picture leaves geotagging information, which gives out the location where that picture was taken. Making phone calls or using short messaging services (SMS) involves cell towers which give locations determining where calls or SMS were sent from. Using global positioning services (GPS) gives away individuals' real time positions along with where they may have been in the past. Wi-fi connections also give

individual locations away. Different functions mobile smartphones devices offer can cause security and privacy concerns for users.

Not only can these concerns be exploited by criminals and hackers, but also law enforcement can use these devices to help them solve criminal cases, which has now become the norm in criminal investigations. Smartphones are one of the most sought-after digital pieces of evidence law enforcement looks for when a crime has taken place, because of all the information they can retrieve from them, without even questioning the suspected individuals. According to Tamma et al. (2018), modern mobile platforms contain built-in security features to protect user data and privacy. These built-in security features continue to be upgraded with each device or software patch released. With each upgrade, there still lacks specific laws that govern digital forensics, which leaves investigators to rely on precedent cases and predetermined laws.

Legal Laws

Fourth Amendment

The Fourth Amendment has been debated in courts for decades and will continue to be debated as interpretation will always be an issue when dealing with individuals' rights. Katz v. United States, 389 U.S. 347, 357 (1967) is where the courts originally held that the Fourth Amendment protection would be triggered whenever the government invaded a citizen's reasonable expectation of privacy. This case followed the previous Supreme Court Trespass Doctrine, where they held that trespass onto a defendant’s property was not enough to warrant Fourth Amendment protection in 1924 (Miraldi, 1977, p. 710).

The Trespass Doctrine was based on physical contact with an individual and/or their property. This, however, would need to be expanded on because emerging technology that law enforcement were beginning to utilize in order to circumvent having to physically be on someone property to collect evidence.

United States v. New York Telephone Company

United States v. New York Telephone Company 434 U.S. 159 (1977) allowed law enforcement get court orders facing telephone companies to install pen registers to record phone numbers dialed on a certain device. The court said that requiring the telephone companies help law enforcement with pen registers would not affect their business operations, as they currently use the method for themselves regularly. This is one of the many cases that the FBI cited in their fight with Apple in 2016.

Kyllo v. United States

Kyllo v. United States 533 U.S. 27 (2001) case revolves around whether the use of a thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within the home constitutes a "search" within the meaning of the Fourth Amendment. In simpler terms, the question the case seeked to answer in general was if the use of technology enhancement tools invaded and/or trespassed on individuals rights within the Fourth Amendment. The government claimed that use of technology should not be considered a search since they did not physically access the defendants' property.

Kyllo, the defendant in the case argued that the government did in fact invade his Fourth Amendment rights by utilizing invasive technology not readily available to the public to look inside his dwelling unlawfully. This is not the first time a case like this has

been heard in front of the U.S. Supreme Court. “Courts have approved warrantless visual surveillance of a home, see California v. Ciraolo, 476 U.S. 207, 213, ruling that visual observation is no “search” at all, see *Dow Chemical Co. v. United States*, 476 U.S. 227, 234—235, 239” in the past (*Kyllo v United States* 533 U.S. (2001)).

Utilizing precedence from the cases mentioned above, the government argued that they did not in fact invade Kyllo Fourth Amendment rights because they only utilized visual observation. This, however, was not the stance of the Supreme court almost 15 years later. The Supreme court held that use of advanced technology from a public location inside a private residence was considered a search within the Fourth Amendment in therefore unlawfully without a warrant.

This holding however still left a lot of questions on the table regarding advanced technology. After this case, there still lacked a significant articulation on exactly “when technology has crossed the line from a new technology, unavailable in law enforcement searches without a warrant, to existing technology in general public use that courts may not now consider a search at all under the Fourth Amendment” (Adkins, 2002, p. 245-267). This has left room for future cases as technology has and will continue to advance, as seen in the *Riley v. California* case where a smartphone now became the technology being utilized to collect evidence.

Along with mobile phone companies such as Apple and Samsung utilizing encryption methods to protect their customers' privacy, the fourth amendment also helps protect citizens from the government (law enforcement) by not allowing them to search or seize digital evidence without the proper authority. The unlawful search and seizure of

digital evidence, especially searching has played a major role in national cases regarding digital evidence. There have been numerous times where law enforcement may have sought out to search an individual's personal device, however needed that individual to unlock such device because they either did not have proper authority to search the device legally using forensic methods and their forensic methods failed to unlock the device.

Research has shown in the past that law enforcement agencies are willing to do just about anything to retrieve valuable information they believe is located on digital evidence. For example, a case where the FBI forced an individual to unlock their Apple iPhone X utilizing face recognition (Brewster, 2018). This as anyone can imagine caused a lot of outcry from the public as it was seen to be disregarding the individual's 4th and 5th amendment rights. According to Fred Jennings, a senior associate at Tor Ekeland Law "the law is not well formed to provide the intuitive protections people think about when they're using a Face ID unlock," (Brewster, 2018). Utilizing intrusive methods to gain access to pertinent information without physically trespassing on individual's property has been debated for decades. Cases such as this have come up more and more often with technology continuing to advance.

Riley v. California

Riley v. California 573 U.S _ (2014) was one of the most notorious Supreme Court Cases dealing with electronic evidence and privacy. This case also revolves around the Fourth Amendment and law enforcement authority to perform warrantless searches on individuals cell phones at the time of an arrest. Riley, the defendant in this case, accused the San Diego Police Department of violating his privacy rights when handing

his personal property and technology. The courts were tasked with deciding two different things within this case:

1. Whether the Fourth Amendment permits police officers to conduct a warrantless search of the digital contents of an individual cell phone, and
2. If so, under what circumstances do they have this authority (Bensur and Brokamp, n.d.).

Two of the key factors weighed for this case was the issue of privacy versus safety. There has been very limited case law dealing with the matter in the digital age before this case. When cellphones (smartphones) become more and more a part of individuals lives, the amount of information on these devices are becoming unlimited access to individuals' livelihoods. Most smartphones nowadays have the same capabilities of computers and why the authority to search someone's computers only comes with a warrant, smartphones have not been properly addressed yet concerning the matter. There have been numerous arguments from groups all around the United States pleading for action to be taken on the matter, however this case was one of the first times the U.S. Supreme Court decided to address the issue.

Law enforcement sees issues with having to obtain a warrant when dealing with smartphones, citing officer safety issues in this case. Per California, smartphones can be rigged to detonate remotely or explode when a specific action is carried out on the phone while in the owner’s possession (Bensur and Brokamp, n.d.). This concern has become very apparent throughout the world with the amount of terrorism that has evolved “Improvised Explosive Devices" (IED), i.e., the Boston Marathon Bombing the year prior

to this case. Another concern for law enforcement is the possibility of individuals being able to delete valuable information or evidence if they are not able to confiscate the devices without a warrant. They also argued that the same information that can be found on smartphones can also be found on pieces of paper, in photographs, in wallets and purses, there is no difference between them searching that information incident to arrest (Bensur and Brokamp, n.d.). The only difference law enforcement sees in the evidence is the form of which it is stored.

After going over all evidence presented during previous trials and cases, the U.S. Supreme Court held that law enforcement would need a warrant to search individuals' smartphone search incident to arrest. The following was concluded:

> Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon—say, to determine whether there is a razor blade hidden between the phone and its case. Once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one. (Riley v California, US 537 (2014))

This decision has set a precedent for future cases to come concerning the digital age and world we live in.

FBI v. Apple

In December 2015, the attack in San Bernardino, CA created a very important discussion regarding national security and individual's privacy rights between the FBI

and Apple. The dispute arose from an application that the FBI filed in a federal magistrate court in California, looking for assistance in the search of an iPhone that was seized from the attack in San Bernardino (EPIC, n.d). This device was originally owned by the San Bernardino Health Department but utilized by the suspect in the 2015 attack. The FBI had tried to unlock the iPhone 5c device themselves with no luck and reached out to the National Security Agency (NSA) for assistance, however they too said they could not access the device.

The application the FBI filed in court asked for Apple to be compelled to create a backdoor for the device for them to gain access to the data located within it. According to the San Bernardino District Attorney on the case, "the phone may house a "dormant cyber pathogen" that threatens the county" (Russell, 2016). The application under the All-Writs Act, 28 U.S.C. § 1651, was granted, however Apple pushed back on the decision, calling it unlawful and unconstitutional. After being granted their order, the FBI got the documents unsealed and notified the press of its request of Apple to assist with the case, however Tim Cook, Apple CEO released a letter to his customers stating he would oppose the order (EPIC, n.d.).

When Apple fought back by filling their own court orders asking to not be compelled to the previous order because of the precedent it could set, the courts began to take another look at the issues. During this time, the FBI was still trying to different ways gain access to the device without Apple helps. They eventually found a third-party company that was able to gain access to the device and dropped the court order on Apple for the time being. It has been discussed that the Israeli company Cellebrite help the FBI,

however the FBI has repeatedly denied this accusation to the public and instead have utilized hackers to create zero-day vulnerability to bypass its ten-try limitation access.

In January 2020, FBI was once again going to go back to court with Apple over the December 2019 shooting at the Naval Air Station in Pensacola, FL. Just like the San Bernardino iPhone access issue, the FBI once again was having problems gaining access to the suspects device in Pensacola. Apple again fought back stating that "it's not about the phones — it's about a year's long push by the Department of Justice for broader government oversight of mobile technology" (Caballero-Reynolds, 2020). This push has continuously affected the world of digital forensics/mobile forensics.

Digital Forensics

Digital forensics has become one of the most complex sciences within the forensic field all together. It has branched off too many different fields that all come with their own complexity to them. When thinking about the field of digital forensics, most individuals are more aware of computer forensics as this was the biggest aspects of the digital forensics when it first came about. Computers, however, have become just one aspect of the field, that now consist of "any devices that store data. "Computers, laptops, smartphones, thumb drives, memory cards external hard drives are within the ambit of digital forensics" (Singh & Kent, 2018).

Other pieces of digital evidence that may not be as obvious to some would be game consoles, fit bits, IoT devices and smart tv's. All these devices can potentially hold some type of evidence for a case that could help solve a crime.

Examiners who work in the field must have special skills sets that they must keep up to date regularly as things change so frequent. They also must familiarize themselves with the many tools that are available to them. These tools can consist of Magnet Forensics, Cellebrite, Oxygen, GrayKey Blackbag and Encase and plenty more.

All these tools serve their purpose in the digital forensic field; however, the most common tools law enforcement tend to utilize for mobile forensic would be Cellebrite and GrayKey.

Cellebrite

Cellebrite is one of the most common mobile forensic tools available to digital forensic examiners. Originally it was created in 1999 for wireless carriers to be able to transfer data from one cellular device to another for its customers. These companies still utilize the tool for this method today, while examiners use it for investigations. In 2007 however, the company decided to expand into the digital forensic field by creating the Universal Forensic Extraction Device (UFED), to help mobile forensics examiners extract data off devices that were encrypted.

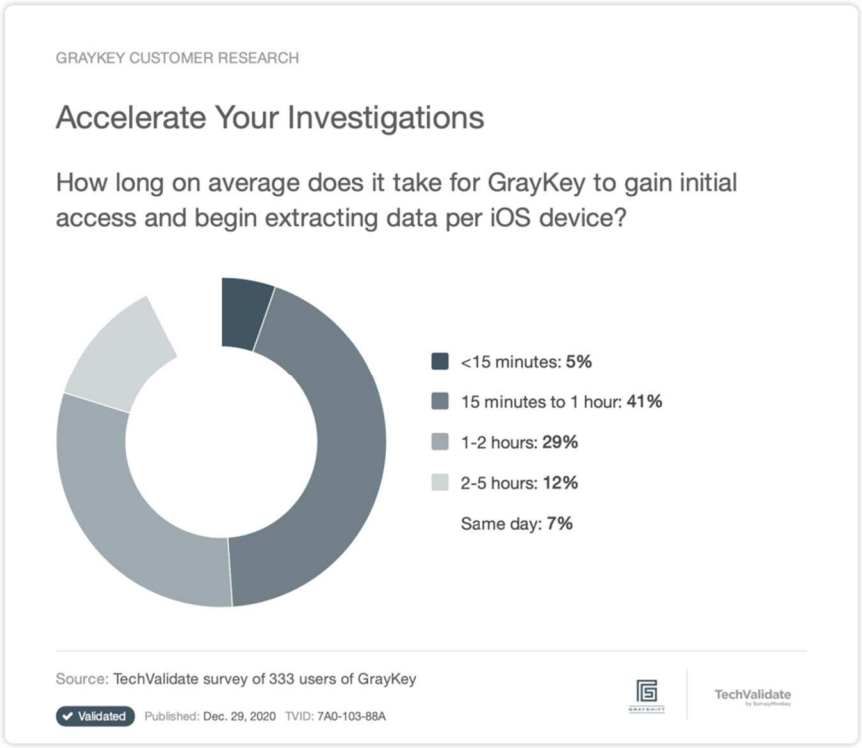
UFED's can be found in just about all local police stations along with their patrol cars now days, as it has become the go to method for law enforcement when acquiring get data from mobile devices. It is a very technology friendly tool that doesn't call for individuals to be experts at mobile forensics, as a lot of times they can just plug the device in and follow the instructions on the device and retrieve the information they are looking for.

GrayKey

GrayKey is one of the most sought-after mobile forensics tools created by the company GrayShift, that is only available to law enforcement and some government entities. This has called a lot of frustration within the mobile forensic field, as examiners with private companies would also like to utilize the tool, however, are not afforded the same opportunities. Defense attorneys run into this issue a lot as they are also not allowed to utilize the tool but have to defend their client from evidence, they are not completely sure how it was retrieved. According to GrayShift, "only GrayKey can provide lawful same-day access to the latest iOS devices in less than one hour" (GrayShift, n.d.).

Figure 1

GrayKey Customer Research



To a lot of mobile forensic examiners and defense attorneys, not having access to tools like GrayKey completely limits their investigations, as this tool has the ability to access a lot of iOS devices that other tools don't. Mobile phones are an essential piece of digital evidence and not having access to one of the best forensic tools, limits certain investigators during investigations.

Digital Evidence

According to the National Institute of Justice (2016), "digital evidence is information stored or transmitted in binary form that may be relied on in court" (para, 2). In recent years, more and more crimes have been committed utilizing electronics such as computer hard drives, personal digital assistants (PDA), flash cards in digital cameras and smartphones to name a few. These crimes leave behind digital evidence that law enforcement have begun to use in order to solve these same crimes. Most Law Enforcement agencies today have specialty units that constantly work and train on how to gather digital evidence without altering it.

The collection of digital evidence is one of the most crucial steps in an investigation, as if not collected proper it can potentially affect the data located on the devices. In the past when computer was the main digital evidence being collected for investigations, there was only one rule, "pull the plug". This allowed for the examiners to ensure no data would be alter, however they did not account for the data that was going to be lost by just pulling the plug. This eventually led to investigators collecting live digital evidence. With smartphones, it can sometimes be a little more complex, however.

With smartphones being minicomputers basically, investigators not only have to be concerned with alter and/or losing some data. They also have to be cautions of individuals being able to remotely wiping data off devices along with completely locking the devices with too many incorrect passcode attempts. One method that is commonly utilized throughout the digital collection field is “if the phone is on, photograph the screen and place it in a Faraday bag, aluminum foil or signal-blocking container. This will prevent a third party from connecting to the phone and being able to alter what's on it” (Kuzia, 2013).

While digital evidence such as smartphones are sometimes considered the ideal piece of evidence in criminal cases, just retrieving a mobile phone does not make a criminal case any easier to solve. There are significant delays when it deals with conducting forensic on digital evidence. According to Hitchcock, Le-Khac and Scanlon (2016), “A significant bottleneck during an investigation involving digital evidence is the time delay from digital evidence being sent to a specialist Technological Crime Unit (TCU) and the assignment to a forensic analyst to complete the necessary in-depth analysis and reporting”. These delays can cause an even more significant issue when the need for the information on the devices are needed for a pertinent investigation. Another reason behind a lot of delays even after the devices reach the appropriate individuals is the amount of security located on the device itself.

With mobile phones, especially smartphones, comes the difficulty of getting past those built-in security measures on the phone to be able to look at potential evidence. Smartphones are constantly being upgraded with new features and security measures with

the consumers privacy in mind and no regard to the digital forensic investigators. This in some cases can become an even bigger issue when presented in court as evidence as forensic examiners must ensure not to alter any data on the devices during an investigation. This is where the term mobile forensics plays comes to light.

Encryption

Encryption has been around for decades and has been utilized to protect sensitive data from individuals who shouldn't have access to it. According to Loshin and Cobb, there are three different aspects of encryption to include: the data, the encryption engine, and the key management (para. 7, 2020). Key management is very important aspects to encryption because if not managed properly, the key could be easily retrievable, making the encryption useless.

Technology companies have taking encryption to an entirely different level, forcing the field digital forensics, especially mobile forensic to stay up to date on the methods. "Governments and law enforcement officials around the world, particularly in the Five Eyes (FVEY) intelligence alliance, continue to push for encryption backdoors, which they claim are necessary in the interests of national safety and security as criminals and terrorists increasingly communicate via encrypted online services" (Loshin & Cobb, 2020). This is an ongoing battle with technology companies, such as Apple, that has not seen any real progress and has been described as stalemate in the past by U.S. leaders.

Mobile Forensics

Mobile forensics, while relatively unique, is one of the fastest growing digital forensics fields being utilized these days. When dealing with criminal investigations, it

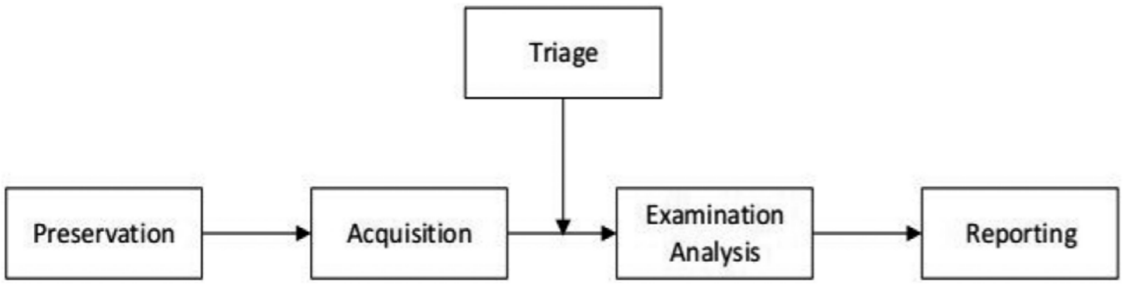
has become very rare to have a case that doesn't consist of some sort of digital forensics with smartphones being one of the most useful pieces of evidence to have. With this evidence comes multiple different processes that should be followed unless the evidence will be considered tainted in a court of law.

According to Tamma et al. (2018) mobile forensics is one aspect of digital forensics that can be broken down into three categories to include: seizure/preservation, acquisition, and examination/analysis.

Each of these categories serve as an important step in the proper handling of digital evidence when conducting criminal cases. There is also an additional category, which is often referred to as the reporting phase where the forensic examiner sums up all their findings in most often a word document. Below shows a limited graph on the sequence of the different phases of mobile forensics:

Figure 2

Mobile Forensic Investigation Process



Seizure/Preservation

Seizure of digital evidence can be one of the most important parts of a criminal case. For law enforcement to first be able to collect/seize digital evidence, they must first

have the proper authority i.e., warrant which can be obtained by a Judge. There are different types of warrants that can be obtained but the most important part of the warrant is where it explains exactly what law enforcement can search and seize as defined within the 4th Amendment. Once digital evidence is seized, it is the responsibility of the investigators to ensure that it is properly preserved before, during and after the investigation.

Preservation of evidence plays a significant role especially when concerning privacy. Digital evidence, especially smartphones can hold an enormous amount of personal information about the owner of the device and if left in the wrong hands that information has the potential of being leaked/exposed. According to Englebrecht et al. (2019) “digital evidence must be stored in such a way that it is secure from unauthorized access by third parties and retains its original condition”. This can become an issue as the focus of the criminal investigation should only focus on certain things, however with digital evidence individuals tend to have to hand over their entire device and not just text messages or photos stored on the phone. Having to relinquish an entire device gives investigators the opportunity to acquire everything within the device during what is called the acquisition of the device, which can be done multiple different days.

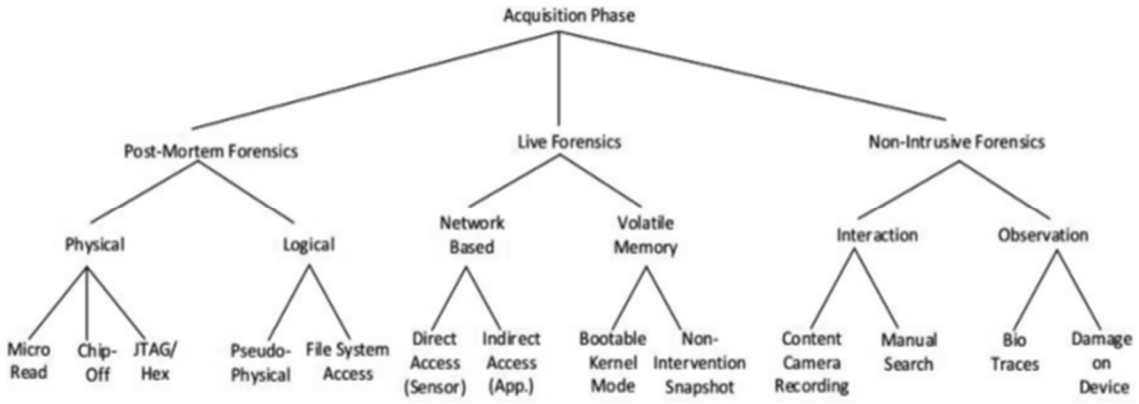
Acquisition

The acquisition phase of mobile forensics can be broken down into three different forensic methods, which all come with a unique advantage and disadvantage. With most users having some sort of security function enabled on their device, whether it be face

recognition, pins or passwords, forensics investigators typically must find ways to bypass these measures without altering any data.

Figure 3

Acquisition Phase



Post-Mortem Forensics is typically used throughout investigations to extract data off devices. Forensic investigators often prefer to get what is called a physical extraction as it affords them more data than a logical extraction. According to Krishnan et al. (2019), physical extraction methods like Hex Dumping, Joint Test Action Group (JTAG), Chip-Off and Micro Read allow for a more direct access to the raw information stored on the smartphone device flash memory. This type of access has the potential to take hours to finish, which the investigator typically has no control over. The investigator also has no control over if the data extraction completely grabs all the necessary data and this will not be known until the extraction is completed, as there is no ability to check while the extraction is taking place. This in turn leaves it up to the actual examination of data to know if all pertinent data was collected.

Examination/Analysis

Examining data after a data extraction is completed can be done in a variety of ways, however this can have its disadvantages. According to Krishnan et al. (2019), there still lacks any global standardization regarding forensic processes and the only framework that lists any type of requirements to be met is the "Smartphone Tool Specifications Standard" developed by NIST. Having standardized guidelines established would make the digital field more comprehensive to the courts. This can be difficult however, as with most things' technology, it is an ever-changing field that is constantly evolving and forcing examiners to continue to find new ways to conduct forensic.

During the examination stage of a mobile/smartphone, investigators must first check to ensure that the data collected was not corrupted during the acquisition phase. This is typically done by making sure there are no blank sectors of data, which is usually identified by the forensic tool utilized to acquire the data. Investigators also need to ensure they are conducting their examination of the data with the acquired copy of the image and not the original.

Depending on the type of investigation the examiner is working on, they tend to tailor what they look for during the examination. If examiners were to look at every piece of data located on the phone, it would take them weeks, sometimes months to go through everything. Forensic tools such as Oxygen have the capability to collect a lot of different information that examiners tend to look at. This information can include, but is not limited to Device Information, Contacts, Call Logs (Missed/Outgoing/Incoming Calls),

Organizer Data (Memos/Tasks/Notes), SMS, MMS, E-Mails, Photos, Videos, Audio and video files, and Deleted Data (Jones & Winster, 2017)

This phase is where privacy becomes an issue for a lot of individuals. As forensic examiners, they have access to everything that is within the phone and this is not comforting for individuals. While examiners may be looking for one thing on a device it is not uncommon for them to find others incriminating or personal information about the device owner. It has been said numerous times that smartphones are an extension of someone's life. According to Nijssen, Schaap and Verheijen (2018), "we rely on our digital devices for doing our jobs, maintaining friendships, navigating traffic, or relaxing after work, and our physical and emotional attachment to them has deepened accordingly".

This information is not something that individuals would likely like to share with forensic examiners, however it is information that examiners would find useful. This is where the corporations such as Apple and Samsung play a significant role in security/privacy. Apple prides itself on its ability to protect its consumers privacy from unwanted parties. Apple Inc, (2021) states the follow on their website:

> Apple believes privacy is a fundamental human right and has numerous built-in controls and options that allow users to decide how and when apps use their information, as well as what information is being used. Your devices are important to so many parts of your life. What you share from those experiences, and who you share it with, should be up to you. We design Apple products to

> protect your privacy and give you control over your information. It's not always easy. But that's the kind of innovation we believe in. (para, 1)

This statement looks to be in line with their reaction in 2016 with the U.S Government. The FBI requested them to unlock or build a backdoor to the iPhone of the San Bernardino shooter and they refused. In an open letter to their customers, Cook (2016) said "The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand" (para, 1).

With the security measures Apple had in place on that device, forensic examiners within the FBI, were having a difficult time acquiring the data on the phone and wanted the company to bypass the security features for them. This would have allowed the examiners the opportunity to conduct an examination/analysis on the device to help build a case against the shooter in San Bernardino. Without Apple's help getting into the device, the FBI worried that there may have been information on the device that would possibly detail another criminal act being planned.

Apple and the FBI are seemingly at odds again with the technology company refusing again to create a backdoor for the law enforcement agency to get into the iPhone of the excused mass shooter in Pensacola, Fl at the Naval Air Station. The United States Attorney General publicly asked Apple to help with the unlocking of the device, while Apple declined and instead assembled a team of advisers to defend their encryption policies as they believe another legal battle with the Department of Justice looms (Hauk, 2020).

Issues such as these will continue to arise when dealing with digital forensics, privacy, law enforcement and technology corporations. Technology corporations continue to expand and upgrade their security features for their consumers; however, this makes the job of a forensic examiner harder daily. Once a forensic tool is developed to bypass one security feature, another security feature is developed to withstand that forensic tool. This is an ongoing battle that appears to have no end in sight and examiners must continue to if not stay ahead of security measures, or at least be up to date with them. If not, their reports are going to be filled with failed attempts at acquiring smartphone data for investigations along with battling technology corporations for help.

Reporting

The report of a digital forensic investigation is one of the most important aspects of the investigation. This is where the examiner explains all the methods utilized throughout the process, how they acquired the data and exactly what data was found on the devices. This report must explain the exact forensically sound investigation methods used for the information found to be used in a court of law. This can sometimes fall short of explaining the forensically sound methods used however, when it comes to law enforcement and their use of the GrayKey tool. As mentioned previously, this tool is not widely available, and its exact capabilities are kept amongst those who are allowed to utilize the tool.

Summary

In this chapter, I discussed the Fourth Amendment which is one of the most important aspect to citizens and the government when it deals with the right to privacy.

Building off Fourth Amendments foundation of privacy, I looked at previous case law where the Courts were forced to step in and make decisions concerning the use of advance technology. Their decision often left room for more discussion because law enforcement methods continued to advance along with technology and prior law left room for interpretation on the issue. It was also discussed within this chapter the daily task and frustrations forensic examiners face while trying to conduct their jobs.

I looked at the different types of digital evidence that can acquired, while also discussing the tools used to acquire such evidence during investigations. Regarding tools used, I talked about how the forensic tool GrayKey can only be access by law enforcement and some government entities. This often can hinder others from conducting complete investigations or defending their clients in court.

From researched literature utilized within this chapter, it appeared to be a common theme that forensic examiners were struggling to keep up with the technology companies regarding encryption and it appears that no one knows how to approach the issue. These themes are in line with other research studies that utilized the phenomenology theory to gain insight to participants perceptions. As mentioned by Miner-Romanoff (2012), Husserl theory can be underutilized when it comes to crime and this research study seeks to clarify why it can be useful.

Using Walden University Library, Google Scholar and Lexis Nexis, I was able to find articles, papers, and court documents by using key search terms. These key terms enabled me to find information regarding struggles forensic examiners are facing. This study will address that issue via interviews with individuals on this topic.

Chapter 3: Methodology

Introduction

This chapter includes the methodology that was utilized to understand the perceptions of mobile forensic investigators concerning, privacy rights, encryptions, and national security. I will also discuss the methods used to collect and analyzed the data from the research conducted.

Interviews of participants involve how important they feel privacy and national security can or cannot coexist together, and if so, the complications involved with this coexistence. Participants were asked to sign consent forms and sit down for one-on-one interviews and/or focus groups to discuss the topic. They also filled out outside activity forms, which is an internal form required by my agency to conduct interviews with individuals I work with.

Research Design

This study was conducted as a qualitative study, which allowed for perceptions of mobile forensic investigators regarding privacy of individuals to be explored. Using the phenomenology theory, this study filled in gaps regarding a subject that had not been thoroughly discussed. This allowed participants to be able to give their opinions in a manner that was thoroughly evaluated.

Role of the Researcher

For this case study, I was the sole researcher and data collector. I was responsible for finding all participants, along with setting up the one-on-one interviews with these individuals. Along with conducting interviews, I created a list of questions each

participant was asked and the order they were asked in. This consisted of open-ended questions that were used throughout the interview. Ensuring that any form of bias on my part was properly addressed and avoiding objectivity was also my responsibility, as I am currently a digital forensic examiner and may potentially have to interview individuals I know.

According to Varga-Dobai (2012), objectivity implies that the researcher can distance themselves from subjects observed during the process of research while ensuring delivering questions in a neutral way without influencing participants. Varga-Dobai said the researcher "enters the research arena with no ax to grind, no theory to prove, and no predetermined results to support" (p. 1-17).

In order to ensure confirmability throughout the study, participants' engagement throughout the study was thoroughly documented to allow for objectivity to be addressed. Each participant received the same emails, documents, and access to interview transcriptions throughout the entire process.

Research Questions

The following questions were used:

RQ1: What is the impact of encryption on mobile forensic investigations?

RQ2: When considering national security, what are the perceptions of mobile forensic investigators concerning privacy rights?

Sampling of Participants

I used the phenomenology theory, and it was imperative that I interviewed individuals who had working knowledge of the topic. These individuals include former

law enforcement members, digital forensic examiners, and attorneys in digital forensics. This selection process is typically called purposive sampling, which is described as selecting individuals who have experience or qualifications with the phenomenon under investigation (Creswell, 2005, p. 204). The goal was to interview 10 individuals, as it became difficult to schedule interviews with individuals who work busy schedules and lacked free time to participate in interviews. As it became difficult to recruit individuals within the law enforcement filed, especially from the FBI, I expanded my research to forensic examiners in general to find available and willing participants.

Data Collection

Sources of data for this study were phone and video interviews during times that were agreed upon by me and participants who willingly participated in the research study. The recording device that was used was checked before each interview to ensure it was working properly. If the recording device was found to not be working properly, a spare was available. If for any reason the spare recording device malfunctioned, I would take notes manually by hand, as myself and the participant would potentially not want to reschedule the interview for a later date. This would ensure the process ran as smoothly as possible. When conducting these interviews, it was imperative to ensure participants felt comfortable throughout the entire interview process and research study. According to Rubin and Rubin (2005), making sure to have a welcoming atmosphere, open dialogue, not imposing perspectives or opinions during conversations, and maintaining flexibility in terms of the flow of interviews are very important.

Interviews started with participants and me going over the informed consent form that was previously emailed to them. This form outlined reasons for the study, what the study will be used for, who had access to the study, and how their opinions would be relayed. Each participant was given the option to maintain complete anonymity to protect their privacy, as their opinions could have the potential to affect their work lives. Participants were also once again informed during any point throughout the interview, if they felt uncomfortable to let me know, and we could discuss whether it would be best for them to withdraw from the study. After going over the consent form, participants were given the option to engage in small talk to help open the conversation in a relaxing manner.

Each interview was expected to last no longer than one hour from start to finish, including time after for questions and summarizing discussions, which was more than enough time. This helped ensure that all information collected was correct and there were no misunderstood questions. During the summary, participants were given the opportunity to ask questions about the actual study that were interesting to them or came to their mind during the questioning stage that they did not get a chance to ask.

All interview questions were derived from the main two research questions to ensure that topics were clearly aligned. Each participant was asked the same questions in the same order to ensure consistency throughout the study. Any follow-up questions were based on answers received from participants.

Reliability and Validity

When considering reliability and validity, individuals tend to connect to the terms to quantitative studies more than qualitative studies. Validity and reliability are two factors which any qualitative researcher should be concerned about while designing a study, analyzing results and judging the quality of the study (Golafshani, 2003; Patton, 2001). An important aspect of reliability and validity is to ensure to incorporate triangulation and member checking within this research study.

Member checking was completed after every interview to ensure information interpretation was complete, by doing a quick summarize of what was discussed. This enabled me to limit the amount time I took from the participants, by not having to reach back out (unless necessary) after the interviews were completed. As mentioned earlier within this chapter the participants may have very limited time to participate, so ensuring to get all information and clarification at the same time is imperative. Triangulation was accomplished by interviewing two different forensic examiners groups. This will ensure to keep my professional beliefs of the topic at bay as participants will have different backgrounds on the topic.

Data Analysis

Data was analyzed by me utilizing narrative analysis. Narrative analysis captures personal and human dimensions of experience over time and takes account of the relationship between individual experience and cultural context (WordPress, n.d, para, 1). Taking in account participants personal experiences and cultural context regarding the

research topic allowed for the data to be thoroughly comprehended. Ensuring data was comprehended correctly, recordings from the interviews were transcribed.

Transcription was completed by me to save on time and money, as transcribing became very costly to get it done professional. This however did make the process a little slower. "At first glance, it might appear that capturing what is said on paper is a straightforward task, however even fairly 'accurate' ones, can be misleading" (Hepburn & Bolden, 2017). After the transcribing of the data, the analysis of the transcribes was thoroughly considered for the most important data to be pulled out utilizing the coding method.

According to Bazeley (2007), coding is one of several methods of working with and building knowledge about data; used in conjunction with annotating, memoing, linking and modeling. Coding can be very complex depending on the data that is being coded, therefore it is important to completely understand the method being utilized. "Any researcher who wishes to become proficient at doing qualitative analysis must learn to code well and easily. The excellence of the research rests in large part on the excellence of the coding" (Strauss, 1987). In order to accomplish the coding, the Nvivo software was going to be utilized as it is designed for data is in word form to help with organization, however I later decided to complete the coding myself without the software. While member checking during the interview phase should clear up any discrepancies, there were instances when I had to get more clarification for the participants. Which was addressed with the individual who was interviewed. If any discrepancies arose during

other phases of the research study i.e., transcribing, I was prepared to address the matter by officially hiring professionals.

Ethical Protections

Staying in line with Walden University requirements for research studies regarding human participant interactions, I obtained approval from the Institutional Review Board at Walden and from the participants who employers required it. I did end up interviewing an individual who worked at the same employer as me, however we have never interacted with each other as our employer has over thousands of workers worldwide. Being proactive, approval was already granted from my employer to speak with individuals, with the acknowledgment of paperwork that was to be filled out prior to any interview. Each participant was required to sign an informed consent (via email) as mentioned earlier and such form will be thoroughly reviewed with the participants before the interviews begin.

Participants were only referenced by numbers, and job titles instead names. Also, their employer's information was not mentioned within the study. After the research study was completed, all data is being kept for a minimum of five years within a lock safe at a location only accessible be myself. After the five years, data will be destroyed utilizing a sound method i.e., wiping the hard drive or completely degaussing it and shredding any physical documents that notes were written on.

With the acknowledgment of interviewing an individual that worked for the same Agency as me, there stood the possibility of conflict of interest that was addressed appropriately from the beginning. This conflict was addressed by ensuring not to go into

too much detail of any particular case or situation the examiner may have dealt with, which alleviated the possibility of any need-to-know information being released within the study.

Summary

Within this chapter, I discussed the methods on how the research would be conducted in order to gather the necessary opinions on security and privacy when it deals with digital forensic. The importance of my role as the researcher and how bias can play a negative role during the interview process. This also comes into play when deciding on who will participate within the research study as only a particular group would comprehend the subject matter. The method of how data was collected and the manner and how it was analyzed, was also discussed within this chapter to give a better understanding of the process. In Chapter 4, the results for the research study will be explained.

Chapter 4: Results

Introduction

In this chapter, I summarize results acquired from participants interviewed for this research. Participants were all asked the same questions involving their opinions or previous and current experience with the topic. Research was conducted by interviewing 10 individuals with digital forensic and specifically mobile forensic experience. These interviews were conducted via Zoom video chat or Microsoft Teams. Each interview was held at a convenient time for the participant and lasted between 30 and 60 minutes. After all interviews were completed, data were transcribed by me to address all relevant information.

After transcriptions of interviews, summaries were sent to everyone via email. Participants returned their summaries with necessary changes that needed to be made along with any additions they wanted added to their interview via member-checking. After this, I analyzed data for common and uncommon themes.

I also discuss demographics of participants within the study. Participants were asked specific questions that only related to them. Gender limitations were also mentioned as it became clear that the study would have more men than women, as technology careers such digital forensics are commonly dominated by men.

Study Overview

The purpose of this study was to understand the issues mobile forensic investigators have while trying to conduct their jobs. As smartphones have continued to advance, encryption has also advanced. With the advancement of encryption methods,

forensic examiners are constantly being tasked with finding new and innovative ways to bypass securities features on their devices. This has led to difficult and sometimes failed attempts, as seen with the FBI in 2016 regarding their efforts to unlock a suspected shooter's iPhone device.

In 2014, former director of the FBI James Comey expressed that allowing the government access to cell phones would enable them to catch not only criminals but also terrorists (Gu, 2014). The theory behind this was that by not allowing U.S. government agencies access to devices, no justice could be served in criminal cases. He fought this stance by indicating that they were not requesting backdoor but rather front door access to be as transparent with U.S. citizens as possible. This, however, would open possibilities for criminal hackers to exploit devices also.

Participants' opinions and experiences are expressed throughout research interviews to gain a better understanding of mobile forensic examiners' perceptions of the issue of encryption. From data that were collected via interviews, mobile forensic practitioners were split on these issues, with different opinions between civilians and practitioners. This became even more evident with participants who had previous law enforcement experience, as they were looking at it from three different perspectives.

Personal and Organizational Influences

During the time I began to collect my data, there were different social and justice issues going on within the U.S. centered around law enforcement. During a world pandemic, law enforcement departments were continuously scrutinized by social and

justice groups for the way they handled situations. I believe this could have played a role in how participants within this study addressed certain questions during interviews.

There were multiple times throughout interviews when social justice issues taking place in the U.S. were brought up as examples. This was evident when asking participants if they felt technology companies helping law enforcement would be seen as a privacy concern. Some participants used examples involving how law enforcement is viewed as untrustworthy as well as how technology companies' ability protect individuals' privacy rights.

Data Analysis and Collection Procedures

Information provided throughout interviews, was the basis of data collected for the study. All participants either had some digital forensics knowledge or were digital forensic examiners themselves, with some knowledge and/or experience with mobile forensics. There were 10 participants coming from either the educational, government, or practitioner industries, with some law enforcement experience.

Data were collected via Zoom and Microsoft Teams for interviews, as personal interviews were not feasible during the COVID-19 pandemic. Participants were giving multiple options to select from regarding day and time of interviews. Interviews were held at least once a week, depending on scheduling, as multiple interviews were rescheduled due to unforeseen circumstances. In total, it took about 5 months to find participants, receive their consent, schedule and conduct interviews, and complete member checks.

Originally, I had planned on doing one-on-one face to face interviews along with one focus group. This plan, however, had to be adjusted as the COVID-19 pandemic made it difficult to interview individuals in person and almost impossible to conduct a focus group. Video interviews seemed the best way to collect my data and keep everyone safe, and I cancelled the focus group altogether.

Participants were all asked the same questions in the exact same order, with some follow-up questions based on their answers. These answers were then analyzed for common or uncommon themes.

After completion of interviews, all participants were given the opportunity to ask any additional questions they may have had concerning the study. If there were no additional questions, I explained next steps, which were that I would write up a summary of interviews and send them via email. This gave each participant the opportunity to look over their summaries and make any necessary changes. After making the changes, they emailed me back the updated summary.

With all summaries updated, I proceeded to look over them and compare any similarities that arose from interviews to gain a better understanding of how much privacy and encryption are a cause for concern with examiners. To complete this, I created three bins for RQ1: Encryption Problematic, Encryption not an Issue and Indifference. Out of the 10 participants, only one felt as if encryption was not an issue, while seven felt it was problematic, and two were indifferent about it. I then created two bins based off RQ2 concerning national security and privacy concerns: Overuse of

National Security and Proper Use of National Security. Two participants felt indifferent about overuse of national security.

It became very clear early on after looking over summaries that there were many similar opinions, with some examiners using the same phrases.

There were also differences amongst the participants as some believed that law enforcement has depended on digital evidence to much lately. This opinion mostly came from participants who had some experience working in law enforcement. They typically referenced that before digital forensics became so popular, investigators in law enforcement knocked on doors and pulled surveillance tapes to solve crimes and this method worked just fine back then, cases were still solved.

Participant Demographics

For this research study, participants were asked to provide their demographic information such as: gender, age range and years in occupation (see Table 1).

Table 1

Demographic Group Information

Participants	Gender	Age range	Years in occupation
1	Female	40-50	10
2	Male	40-50	3
3	Male	30-40	4
4	Male	40-50	15
5	Male	50-60	23
6	Male	30-40	5
7	Male	20-30	8
8	Female	30-40	8
9	Male	40-50	18
10	Male	30-40	11

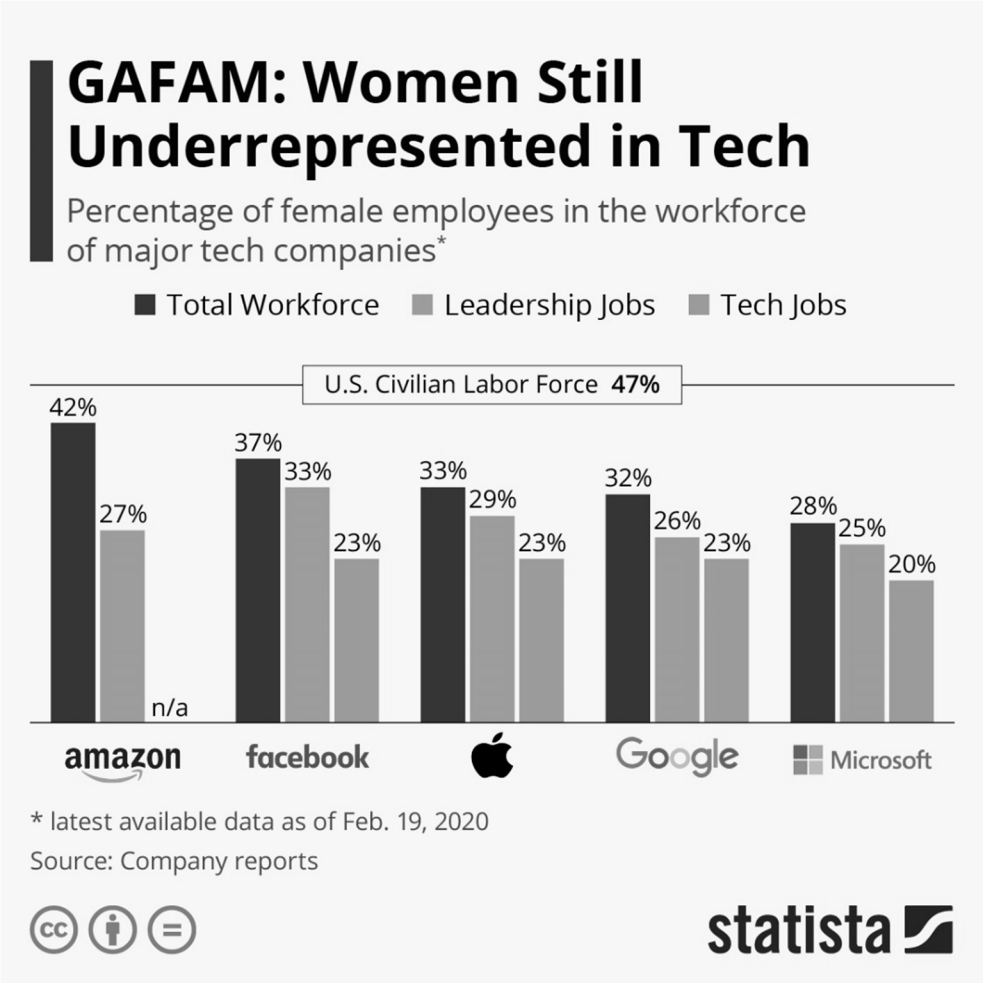
As seen in Table 1, participants had a very wide variety in years worked in the field. Some examiners were new to the field, while others have been in the filed for almost as long as it has existed. The age range tended to lean more towards the 40-50 range, with only one individual being under 30 at the time of the interview. I believe with the variety of differences in years in the field and age, I was able to grasp a good understanding of how individuals feel about the state of mobile forensics.

There was also a clear lopsidedness when it came to gender and this study, as I was able to interview more men than women. The technology field tend to be dominated

by males, with women being like a needle in haystack. The figure below shows how the biggest technology companies in the United States, not only lack women in the organizations, but women in technology.

Figure 4

GAFAM: Women Still Underrepresented in Tech



With the lack of women in the technology field, I went into this study realizing that recruiting mobile forensic examiners would be difficult. I didn't account for the lack

of women however, and only realized this issue once I began finding willing participants that were majority men.

Interview Data

Participant 1

Participant 1 was a practitioner/educator within the field currently and has been doing the digital/mobile forensic for 10 years.

> She stated that encryption on mobile devices is not that much of a concern as many people may believe. Examiners have the full device in their possession during an investigation, which hold the keys on them. Encryption can still be a technically challenge those examiners must consistently overcome and have overcame for the past decade by thinking outside the box. It is a game of cat and mouse, that is to be expected in the technical field. Protecting privacy and allowing for legal acquisitions of content should be a partnership.
>
> The bigger concern would be wipe capabilities that technology these days have.

Participant 2

Participant 2 worked for the government as a practitioner in the field and has been doing digital/mobile forensic for 3 years.

Regarding whether or not law enforcement should be able to search devices search incident to arrest, the participant had the follow to say:

> This depends on why the individual was original stopped. There was an incident close to where I reside, that law enforcement pulled over a vehicle and the occupant of the vehicle had committed a murder and was arrested. If allowed to

> go through the individual's device the officers could have possible retrieved evidence of the murder. While I do not believe that law enforcement should be allowed to go through everyone's device without probable cause, there is times I feel as if they should be allowed.

The participant also believed that current, Apple iOS devices are more difficult to gain access to then Googles, Android devices. Stating that Apple's source is more protected then.

Participant 3

Participant 3 worked for the government as a practitioner in the field and has been doing digital forensic for 10 years and mobile forensic for 4 years. He has taking multiple courses regarding mobile forensic to include a chip off course.

He believed that technology companies' encryption methods absolutely hinder mobile forensics. For example, with the iPhone version 4 and up, it's almost impossible to get a physical capture of it. While you can jailbreak or root an Android device to obtain a physical dump, doing so also mean you are altering evidence, which in turns complicates things. He noted the following regarding the overall issues tech companies and law enforcement have:

> At the end of the day, there needs to be something done, some type of communication between mobile forensic examiners and tech companies regarding working to together. There should be clear an understanding between both. Companies such as Apple should be held accountable for not wanting to work with law enforcement, especially when there is an incident where there is a loss of

> life. The news and media also play a role in such situations, as they often relay the message to the public that law enforcement is trying to access private information from devices, when in reality they are only trying to take preventative measures to stop incidents such as San Bernardino.

Participant 4

Participant 4 worked for the government as a practitioner in the field and has been doing digital/mobile forensic for 15 years. He noted the following:

> Apple devices tend to be more difficult to access for mobile forensic examiners than Android right now regarding encryption methods. Apples are narrower targets, unlike Android devices. Android might have the similar base OS, but the implementation may be different, and examiners may just get lucky utilizing a random technique, unlike Apple devices which are better put together. … At the end of the day, this will be a losing battle for both sides, because if law enforcement does get technology companies to work with them, technology companies are going to provide an encrypted blob that law enforcement is still going to have issues with decrypting. As a private citizen, I have no issues with this because the government shouldn't be allowed to just access my information when they want to.

Participant 5

Participant 5 has worked in the digital forensic field for over 23 years and is a certified mobile forensic instructor. He has experience with teaching mobile forensic to law enforcement and government individuals. He noted the following:

> Regarding tech companies helping or not helping law enforcement access smartphones, speaking from a private citizen perspective, tech companies have a duty to provide its consumers with secure devices that do not have backdoors that the government would be able to access. However, as a retired law enforcement officer, I believe tech companies should help with accessing smartphones. Overall, I see privacy as a big concern with big tech, as it's being comprised for marketing purposes. … It would be a privacy concern for citizens if technology companies freely help law enforcement with their forensic investigations. Citizens have an expectation of privacy, and their personal data should be secured. Individuals are getting so attached to their smartphones that they are becoming an extension to themselves. I believe law enforcement is utilizing smartphones as an easy way of conducting investigations, instead of getting out there and investigating crimes now days. Before smartphones existed, crimes were being committed and solved, therefore they should still be able to solve crimes today without invading individuals' privacy by accessing their smartphones.

Participant 6

Participant 6 is an attorney for the local public defender office, who works closely with the mobile forensic examiners. He also has experience with testifying in court regarding mobile forensic. He noted the following:

> Technology companies should never help build a backdoor into encryption for law enforcement or anyone else, because it would be a terrible precedent to set. Law enforcement has failed to show how that exploit wouldn't put the consumers

of that product at risk from others trying to exploit that same vulnerability. If you intentionally put in a backdoor, other people who you didn't intend on walking through will walk through it as well. … Technology companies helping law enforcement during investigations will be a privacy concern, especially when considering exactly what the technology companies are doing to assist. I feel citizen have less of an argument when thinking about privacy when it comes to social media such as Facebook. It would be naive to believe that such companies are not going to turn over personal information to law enforcement if they have a lawful warrant. … My concern is that technology companies are less willing to challenge law enforcement compared to other departments. Attorneys can't just subpoena information from companies like Facebook, Google etc... they are prevented by a Federal Law called Stored Communications Act (18 U.S.C. §§ 2701–2712). It is antiquated law that has been used to prevent defense attorneys (and anyone who isn't law enforcement) from being able to gain access to or copies of social media data/records, emails, etc. Also, even when requesting information attorneys are legally allowed to have, those same companies will fight tooth and nail to not provide such information but will bend over backwards for law enforcement. There is a little bit of imbalance when it comes to who certain companies are more willing to help.

Participant 7

Participant 7 is a digital forensic examiner for a local/state defenders office, who has 6 years' experience with mobile forensics. He noted the following regarding technology companies helping law enforcement:

> Coming from an examiner perspective I think it would be a privacy concern for the public especially for individuals who are technology educated. For example, if Apple decides they are going to help law enforcement 100% of the time and Google decide they are going to help on a case-by-case situation, most people will decide to utilize Google, since they are working harder to protect its consumers privacy rights. For your everyday person, who is not that aware of how technology works, I still think it would be a privacy concern also. For example, no one wants Facebook giving out all their information, so why would we want a phone manufacturer to do the same thing.

In regard to the 4th amendment applying to individuals' personal devices, participant 7 expressed the following:

> The 4th amendment should apply to individual's personal media devices just the same as it does to dwelling or person. Smartphones have become part of who individuals are now and just about everyone has one. Law enforcement shouldn't be able to search a device without the proper authority, just as if they wanted to search someone's dwelling.

Participant 8

Participant 8 is also a digital forensic examiner for a local/state defenders office, who has 8 years' experience with mobile forensics. She noted the following:

> Technology companies' encryption methods can hinder mobile forensic investigations as seen with the San Bernardino incident, where the FBI felt they needed Apples help but ultimately utilized a third-party company to gain access to the iPhone. There are two main companies (GrayShift and Cellebrite) that work to circumvent encryption methods on iPhones, but they are not perfect and don't work on every model of every phone. Technology companies not helping is not a complete roadblock, but there are times where examiners can help a dead end and not be able to access a device and retrieve the data from it.

He had this to say when asking about a solution to the issues between law enforcement and mobile forensic examiners:

> I do not believe tech companies should just blindly help law enforcement without a lawful court order telling them to. The same way law enforcement uses warrants to make companies like Apple turn over individuals iCloud backups, there should be no difference in them when trying to get access to the actual devices.

Participant 9

Participant 9 has over 18 years of experience with not only digital forensics, but mobile forensics as well. He conducted mobile for forensics while working in law enforcement and is very familiar with the field from when it was just beginning to expand

beyond just computer forensics. Regarding the state of mobile forensics today and privacy he stated the following:

> I think it would be a privacy concern for the public. While I think law enforcement should be able to utilize tools at their disposal if used legally, I don't think the government should be able to tell any of the big tech companies that they have to give them encryption keys to access their devices. There are plenty of examples where the government has not handled their access to data well, they have been breached time and time again. They do not show good cyber hygiene, so why would we trust them with the ability to just reach into anyone device. Once that backdoor is created and is breached by China, Iran, or Russia, they now have that ability to access those devices as well. It is a tough situation and there is not an easy answer.

He also believed the following regarding limiting forensic tools from the private sector:

> The issue I have with the limited access to this tool is that law enforcement is utilizing a tool that no one else has access to and no one can articulate how the tool works, no one can articulate whether it is actually injecting something into that device for it to work correctly. There is not much worse you can do to someone then prosecute them, take away their civil rights and then say, we got all this information about you that we are going to use against you in court, but your defense team or defense experts cannot get access to that, and we can't tell them how we did it. I do not think that's fair, nor do I think that is the intent of our

> constitution when it comes to the ability to present a defense. I would understand more if it was an intelligence specific tool.

Participant 10

Participant 10 has conducting mobile forensics for 11 years, with focus on iOS devices. They have taken multiple courses on the topic and is considered a senior examiner at their organization.

When asked specifically about whether encryption on smartphones can hinder investigations, he had the following to say:

> Encryption has been around for some time now and has only gotten better on smartphones. It can hinder an investigation, because it makes it 10 times harder to access devices, while back in the day it was basically plug and play. Now days, you must bypass so many security measures that when examiners are finally able to access the data on the device it may be too late for the investigation.

When questioned about privacy and whether technology companies should work with law enforcement, he said the following:

> Law enforcement clearly has a job to do and anything to help them complete the job is great. I, however, do believe that forcing technology companies to help law enforcement with their investigations may be stepping over the line. If technology companies decided they wanted to help law enforcement, then great, but I think it should be the technology companies' decision and not the governments.

Themes by Interview Question

Interview Question 1

Are you familiar with the 2016 Supreme Court case Apple v. FBI?

All interviewees were familiar with the 2016 Supreme Court case *FBI v. Apple* in some sort of way. While they all had different understanding or knowledge of the situation and how it related to the San Bernardino incident, the concept of the situation was able to be related to the research study.

Interview Question 2

With the FBI dropping the case, what is your take on tech companies helping or not helping law enforcement in such cases?

Most interviewees felt almost the same regarding this question, while their reasonings may have been a little different. Majority felt as if technology companies had some type of duty to help law enforcement, they did not think it they should blindly help them whenever asked to without proper reasoning.

Interview Question 3

Do you believe that tech companies encryption methods, hinder mobile forensic investigations?

Again, most interviewees felt as if technology companies' encryption methods do hinder mobile forensic investigations, some felt it was not a complete roadblock. A couple also felt as this is not even the biggest issues forensic examiners have to be concerned about.

Interview Question 4

What are your thoughts when considering law enforcement conducting mobile forensic examinations concerning encrypted smartphones?

This question was a very compound question as it was elaborated into utilizing biometrics to unlock devices and deceased individuals right to privacy. All felt that law enforcement should obtain a warrant before being able to access individuals' smartphones, including using biometrics. The divide regarding this amongst the interviewees came when considering individuals who were already deceased.

Most seemed undecided on if they thought law enforcement should be able to use biometrics to unlock smartphones if the individual was deceased. The question of legality came up, with most not knowing what the legal guidelines where regarding deceased individual's privacy rights on their mobile devices and what the courts have to say on the matter.

Interview Question 5

In your opinion, do you believe that if tech companies were to help during investigations, it would be a privacy concern for the public?

Some felt as if this would be of some concern to the public but was not totaling against it happening. They believed that depending on the situation, some individuals would not mind technology companies helping during investigations, however they did not think it should be a normal thing for every case.

Interview Question 6

Regarding social media and privacy, do you think as individuals we give our own privacy away?

Everyone agreed that when it comes to social media and privacy, individuals completely give away so form of their privacy. There were some that felt if individual took an additional step to make their social media accounts private, then they could expect some type of privacy, but not complete from investigations.

Interview Question 7

Do you think national security and privacy can collide with each other?

All felt that national security and privacy can collide with each other, while some felt it collide daily, hence the United States Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Act being created. It was a common theme amongst the participants that law enforcement can sometimes utilize national security as a crutch. Most felt like national security laws were too broad and needed to be looked at again.

Interview Question 8

Are you familiar with the verbiage used within the 4th amendment? If so, can you explain what it means to you?

With a little clarification for some, the 4th amendment was understood and explained how it correlated to this research study.

Interview Question 9

With the 4th amendment protecting individuals from unreasonable search and seizures, what are your thoughts when it comes to individual's personal media equipment?

All agreed that individual's personal media equipment should apply to the 4th amendment with no issues. The key theme within this response was that personal media equipment now days hold a lot of personal information on them, and they should be treated the same as if law enforcement wanted to search an individual private dwelling. Meaning law enforcement should not have unlimited access to individual's personal media devices.

Interview Question 10

What is your opinion regarding the forensic tool GrayKey only being available to law enforcement?

All participants had very strong opinions against this tool being limited to certain individuals. They all felt as if there was no logical reason to have a limit tool when other tools are available to everyone. In their opinions, they felt as if it gave law enforcement an edge that others did not get in the court of law.

Interview Question 11

What is your overall opinion regarding a solution for the issues the FBI and Apple continues to face with each other? Should the courts step in or should law enforcement and technology companies figure out a solution on their own?

This was a very split question amongst the interviewees. Some felt that they did not see how the courts would be able to help the situation, while other felt that their needed to be more rulings on the situation. All felt that law enforcement and technology companies would not be able to come to a comprise, as they both had different agendas in the matter. They also mentioned that there would be no clear resolution with this issue no time soon.

Themes by Research Question

This study consisted of two research questions:

RQ1: What is the impact of encryption on mobile forensic investigations?

RQ2: When considering national security, what are the perceptions of mobile forensic investigators concerning privacy rights?

This section will summarize the study's themes in accordance with the research questions presented.

RQ1

Most participants within the study agreed that the encryption methods on devices affected criminal investigations in different ways. While there was discussion that this was not as big as concern as many may believe. With technology companies constantly coming up with new ways to encrypt their devices to protect the user's privacy, it can sometimes delay mobile forensic examiners investigations. Even with law enforcement having special tools that helps circumvent most devices encryption methods, this still sometimes is not enough for the newer devices, as these tools only work on after they have been introduced to the encryption before.

RQ2

Participants all seemed to come to a common ideology, that when it comes to national security, privacy should potential be altered to a degree. While most didn't mind their privacy being invaded, they only agreed with it if the proper channels were followed, i.e., going through the court system.

Privacy was very important to all participants, but so was national security. Some agreed that technology companies should in fact work with mobile forensic examiners on certain cases, however they did not think they should be forced to by the government. One thing that was very common and obvious throughout all the participants interviews was that there needed to be some checks and balances in place when considering privacy. There also needed to be limitations on how law enforcement utilized national security concerns to circumvent individual's privacy rights during investigations.

Summary

In this chapter, I discussed the results of a phenomenology-based theory regarding mobile forensics and the perception of privacy. Ten individuals from backgrounds ranging from educators to actual practitioners, were afforded the opportunity to give their opinions on mobile forensics and advancing encryption methods by technology companies. Opinions were transcribed and then analyzed for common themes to collect a cohesive conclusion on the data collected.

The interviewed individuals seem to struggle with looking at it from a practitioner perspective and private citizen as their answer were carefully considered. While they all

would like to make life easier for mobile forensics examiners in the field, they also did not want to just give up their privacy rights all together as private citizens.

They tended to agree that something needed to be done, but exactly what, was a very complex issue, as it would take potentially years to come to a full understanding and agreeance with both technology companies and mobile forensic examiners. As multiple participants put it during their interview, it is just a game of cat and mouse at this point, and no one has a solution to make everyone satisfied. In chapter 5, I will discuss future research that can be conducted along with personal reflections and interpretations of my results.

Chapter 5: Conclusions and Recommendations

Introduction

In this chapter, I discuss the results of this qualitative research study to understand effects technology companies' encryption methods have on criminal investigations. I also discuss privacy concerns when considering national security. Questions have been raised in the Department of Justice and amongst technology companies, with there being no clear solution on how to resolve them.

There were 10 individuals who were interviewed, and interviews were structured similarly, with few differences in terms of follow-up questions based off responses that were given to me. These individuals were government workers, educators, and practitioners. With the interview pool being limited, I decided to correlate common themes myself instead of using software.

Results Summary

This study involved exploring a very rare topic that is not often discussed unless something significant happens in the U.S. Participants within this study all agreed that this was an interesting and important topic that has not been clearly addressed. They felt as if governments' demand for technology companies were excessive. Privacy was one the biggest concerns participants had when it came to law enforcement requesting help from technology companies. They believed privacy was important to citizens; however, it is hindered when individuals decide to use social media.

National security was thought to be used too broadly from a law enforcement perspective and should not be used to gain access to individuals' personal media devices.

Participants felt as if the only way law enforcement should be able to gain access to devices is if they went through proper channels such as court orders or consent from the individuals themselves. It was also noted that while law enforcement claims to not be able to access many devices, that is not completely the truth.

They also believed that law enforcement was not honest about data they had access to without getting into devices. Technology companies often comply with court orders to hand over data from their consumers, such as iCloud data on Apple devices. Such data can include mail and text messages. This is not sufficient for law enforcement, however, because this data can still be encrypted, which can leave law enforcement with the same issue as before.

Findings

Recruitment of participants was done via social media sites or LinkedIn in addition to my prior knowledge of them working in the field. This ensured that participants were qualified to speak on the intended topic and comprehended questions being asked during interviews. Based off interviews with participants, I believe that research study addresses an ongoing issue that has not been properly addressed.

The results of the research study confirmed that participants all thought there was an underlying issue with privacy, encryption, and national security, however none had a clear solution on how to address their concerns. I believe this needs to continue to be researched from different perspectives as I only looked at it from mobile forensic examiners' perspectives, which in many cases has limitations.

Limitations

One of the primary limitations of this study involved the small sample size. Participants in this study needed to have knowledge of not only digital but also mobile forensics as well. With only 10 participants, this limited the number of diverse opinions needed to understand how significant the issue is. This study was also very lopsided in terms of gender, as the technology field is heavily saturated with men. While this was not a factor according to examiners, I think this can lead to bias, as the study was completed with a 80/20 split between genders.

Social Change

Timing of such a study is imperative to current situations involving technology companies and the U.S. government. With the increase in domestic terrorism in the U.S., this issue is going to become even more relevant. With individuals using their smartphones for everyday life, these devices are going to become a focal point in criminal cases in more. Technology companies and forensic examiners are often going to be at odds and will eventually have to figure out ways to work together for the greater good of everyone involved.

Social change can be affected by this study in different ways. Enhancing communication between technology companies and mobile forensic examiners when it relates to encryption methods would help in terms of understanding their stances. Encryption methods on smartphone devices will continue to advance as criminals continue to find ways around them.

As technology continues to advance along with encryption methods, I would hope this research study could begin the deep conversations needed between the mobile forensic examiners and technology companies. Using an interpretivist approach, there could be an understanding of both sides. However, until courts decide to address the issue, there will be no clear understanding between technology companies and law enforcement agencies when dealing with privacy.

Recommendations

This qualitative research study was conducted with data from different demographic groups. Other research studies can be conducted involving general public opinions of the matter involving individuals who may have limited experience or knowledge concerning encryption issues. Also, interviewing individuals from technology companies would lead to different perspectives on the topic.

Another option would be to conduct a quantitative study regarding the topic with a much larger participant pool including individuals all over the U.S. The study can be conducted to gather the opinions of the general public and mobile forensic examiners to get a better understanding on how much privacy means to both.

Personal Reflections

Conducting this study allowed me to reflect on a topic that is emerging. Mobile forensics are constantly changing and forcing technology companies to continue to think how to protect its consumers. When conducting this study, I was at the time entering into the field of digital forensics for the government. Being so new to the field afforded me the opportunity to address different angles and views from different examiners. I believe I

was able to understand a multitude of different perspectives no matter where examiners where currently working.

I was able to gain a significant amount of knowledge of the field by interviewing individuals from different backgrounds. I identified certain themes that came about based on where individuals may have worked or currently worked. While timing began to be an issue with interviewing law enforcement, speaking with prior individuals who have worked in law enforcement was just as beneficial because I believed their perspectives on current issues is very important to the topic. The government and private sectors must figure out how to coexist in the data protection realm. If not, this issue will be magnified.

Conclusion

Digital forensics and especially mobile forensics is a field that is getting more complex. Encryption will continue to become more advanced as technology companies seek to find ways to continue to protect their consumers' sensitive data. Eventually a compromise is going to have to happen, whether it comes from the courts or the organizations themselves.

References

Adkins, D. (2002). The Supreme Court announces a Fourth Amendment "general public use" standard for emerging technologies but fails to define it: Kyllo v. United States. *University of Dayton Law Review, 27, 245-267.* https://heinonline.org/HOL/LandingPage?handle=hein.journals/udlr27&div=16&id=&page=

Alawadhi, I. (2019). *Methods and factors affecting digital forensic case management, allocation and completion*. [Doctoral dissertation, University of Central Lancashire]. ScholarWorks. http://clok.uclan.ac.uk/30744/1/30744%20Alawadhi%20Ibtesam%20Final%20e-Thesis%20%28Master%20Copy%29.pdf

Apple Inc. (2021). Privacy. https://www.apple.com/privacy/

Au, M., Choo, K. R., & Kessler, G. C. (2017). *Mobile security and privacy: Advances, challenges and future research directions*. Syngress.

Astalin, P. (2013). Qualitative research designs: A conceptual framework. *International Journal of Social Science & Interdisciplinary Research*, *2*(1), pp. 118-124. https://pdfs.semanticscholar.org/baa7/c8f5577b0b1798b5e9f559f5cbae32bf1a36.pdf

Barmpatsalou, K., Damopoulos, D., Kambourakis, G. & Katos, K. (2013). A critical review of 7 years of mobile device forensics. *Digital Investigation. 10*(4), 323–349. https://doi.org/10.1016/j.diin.2013.10.003

Barmpatsalou, K., Cruz, T., Monteiro, E. & Simoes, P. (2018). Current and future trends in mobile device forensics: A survey. *Association for Computing Machinery*, *51*(3), 1-31. https://doi.org/10.1145/3177847

Bazeley, P. (2007). *Qualitative data analysis with NVivo.* SAGE Publications.

Bensur, G, & Brokamp, J. (n.d.). Riley v. California. https://www.law.cornell.edu/supct/cert/13-132

Blasdel, E. (2010). *A phenomenological study of barriers for women in federal law enforcement* (Publication No. 3506881) [Doctoral dissertation, University of Phoenix]. ProQuest Dissertation and Theses.

Brewster, T. (2018). *Feds Force Suspect to Unlock an Apple iPhone X with Their Face*. https://www.forbes.com/sites/thomasbrewster/2018/09/30/feds-force-suspect-to-unlock-apple-iphone-x-with-their-face/#645c06b61259

Caballero-Reynolds, A. (2020). Two iPhones or the privacy of billions*: Why Apple vs. the FBI matters*. https://www.nbcnews.com/tech/security/two-iphones-or-privacy-billions-why-apple-vs-fbi-matters-n1118001

Cisco (2016). The rise of mobile: 11.6 billion mobile-connected devices by 2020. http://mobilefuture.org/the-rise-of-mobile-11-6-billion-mobile-connecteddevices-by-2020/

Creswell, J. W. (2005). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research.* Pearson Merrill Prentice Hall.

Creswell, J. (2006). Five Qualitative Approaches to Inquiry. https://www.sagepub.com/sites/default/files/upm-binaries/13421_Chapter4.pdf

Cook, T. (2016). A message to our customers. https://www.apple.com/customer-letter/

Dudovskiy, J. (n.d). Interpretivism (interpretivist) Research Philosophy. http://research-methodology.net/research-philosophy/interpretivism/

Dcng, H. (2015). Introduction to Mobile Forensics. *eForensics.*https://eforensicsmag.com/introduction-to-mobile-forensics/

Englbrecht, L., Langner, G., Pernul, G. and Quirchmayr, G. (2019). Enhancing credibility of digital evidence through provenance-based incident response handling. In Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19). *Association for Computing Machinery, New York, NY, USA, 26*, 1–6. https://doi.org/10.1145/3339252.3339275

Electronic Privacy Information Center (n.d.). Apple v. FBI. https://www.epic.org/amicus/crypto/apple/

Gillware. (n.d.). Why mobile forensics? https://www.gillware.com/phone-data-recovery-services/cell-phone-forensics/

Grayshift (n.d.). Speed and Access are Essential. https://www.grayshift.com/graykey/

Griffin, L. (2018). Digital Forensic Imaging: Types & Examples. https://study.com/academy/lesson/digital-forensic-imaging-types-examples.html

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report, 8*(4), 597-606. http://www.nova.edu/ssss/QR/QR8-4/golafshani.pdf

Hack, M. (2016). Feature: The implications of Apple's battle with the FBI. *Network Security*, *2016*8-10. doi:10.1016/S1353-4858(16)30068-X.

Hauk, C. (2020). Apple Gearing Up for Legal Battle with DOJ Over Pensacola Shooter's Locked iPhones. https://www.mactrast.com/2020/01/apple-gearing-up-for-legal-battle-with-doj-over-pensacola-shooters-locked-iphones/

Hepburn, A., & Bolden, G. (2017). *Transcribing for social research*. 55 City Road, SAGE Publications Ltd doi: 10.4135/9781473920460

Hitchcock, B., Le-Khac, N., & Scanlon, M. (2016). Tiered forensic methodology model for Digital Field Triage by Non-Digital Evidence Specialists. *Digital Investigation 16*, pages 75-85, https://doi.org/10.1016/j.diin.2016.01.010

Hosein, G. (2017). Compromising Over Technology, Security, and Privacy Commentary. *International Journal Of Communication*, *11*902-906.

Jones, G.M., & Winster, S.G. (2017). Forensics Analysis On Smart Phones Using Mobile Forensics Tools. *International Journal of Computational Intelligence Research 13*(8), p. 1863. https://www.semanticscholar.org/paper/Forensics-Analysis-On-Smart-Phones-Using-Mobile-Jones-Winster/b8e51c929ee09450ae951e96d95fc294e2da40d7

Katz v. United States, 389 U.S. 347, 357 (1967). https://www.law.cornell.edu/supremecourt/text/389/347

Krishnan, S., & Zhou, B., & An, M. (2019). Smartphone forensic challenges. *International Journal of Computer Science and Security, 13*(5), 183-196. https://www.cscjournals.org/manuscript/Journals/IJCSS/Volume13/Issue5/IJCSS-1501.pdf

Kuzia, G. (2013). Handling Cell Phones and Their Digital. https://www.policemag.com/374289/handling-cell-phones-and-their-digital-evidence

Kyllo v. United States, 533 U.S. 27 (2001). https://www.law.cornell.edu/supct/html/99-8508.ZO.html

Levy, M. S. (2017). Holding the FBI Accountable for Hacking Apple's Software Under the Takings Clause. *American University Law Review*, *66*(5), 1293.

Loshin, P., and Cobb, M. (2020). Data security guide: *Everything you need to know*. https://searchsecurity.techtarget.com/definition/encryption

Interagency Security Committee. (2015). Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide. https://www.dhs.gov/sites/default/files/publications/isc-planning-response-active-shooter-guide-non-fouo-nov-2015-508.pdf

Makin, D. A., & Morczek, A. L. (2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology, 9*(1), 55-119. doi:10.5281/zenodo.22387

Mikhaylov, I. (2017). *Mobile Forensics Cookbook: Data acquisition, extraction, recovery techniques, and investigations using modern forensic tools.* Packt Publishing.

Miner-Romanoff, K. (2012). Interpretive and Critical Phenomenological Crime Studies: A Model Design. *The Qualitative Repor, 17*(54). https://doi.org/10.46743/2160-3715/2012.1756

Miraldi, D. (1977). The Relationship Between Trespass and Fourth Amendment Protection After Katz v. United States. *Ohio State Law Journal 38*(709), 710 https://kb.osu.edu/bitstream/handle/1811/64146/1/OSLJ_V38N3_0709.pdf

Moustakas, C. (1994). *Phenomenological research methods*. Sage.

National Institute of Justice. (2016). Digital Evidence and Forensics. https://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx

Newman, L. (2021). How Law Enforcement Gets Around Your Smartphone's Encryption. https://www.wired.com/story/smartphone-encryption-law-enforcement-tools/

Nijssen, S., Schaap, G., & Verheijen, G. P. (2018). Has your smartphone replaced your brain? Construction and validation of the Extended Mind Questionnaire (XMQ). *PloS One, 13*(8), e0202188. https://doi.org/10.1371/journal.pone.0202188

Richter, F. (2020). GAFAM: Women Still Underrepresented in Tech. https://www.statista.com/chart/4467/female-employees-at-tech-companies/

Riley v. California, 134 S. Ct. 2473 (2014). https://www.law.cornell.edu/supct/cert/13-132

Rubin, H. J., & Rubin, I. S. (2005). Qualitative interviewing: The art of hearing data (2nd ed.). Sage.

Russell, J. (2016). San Bernardino DA claims Syed Farouk's iPhone may house 'cyber pathogen'. https://techcrunch.com/2016/03/03/san-bernardino-da-claims-syed-farouks-iphone-may-house-cyber-pathogen/

Saldana, J. (2016). *The Coding Manual for Qualitative Researchers* (3rd ed.). SAGE Publications.

Singh, A. & Kent, C. (2018). The What, Why, and How of Digital Forensics. *Law Technology Today*. https://www.lawtechnologytoday.org/2018/05/digital-forensics/

Strauss, A. (1987). Qualitative analysis for social scientists. University Press.

Smith, D. W. (2016). "Phenomenology". *The Stanford Encyclopedia of Philosophy.* https://plato.stanford.edu/cgi-bin/encyclopedia/archinfo.cgi?entry=phenomenology

Tamma, R., Skulkin, O., Mahalik, H., & Bommisetty, S. (2018). Practical mobile forensics*: A hands-on guide to mastering mobile forensics for the IOS, Android, and Windows phone platforms.* (3rd ed.). Packt Publishing.

Thanh, N. & Thanh, T. (2015). The Interconnection Between Interpretivist Paradigm and Qualitative Methods in Education. *American Journal of Education Science, 1*(2), 24-27. https://pdfs.semanticscholar.org/79e6/888e672cf2acf8afe2ec21fd42a29b2cbd90.pdf

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

Universal Data Acquisition. (n.d.). Data Acquisition. http://www.forensiccomputerservice.com/general-services/data-acquisition.aspx

Varga-Dobai, K. (2012). The Relationship of Researcher and Participant in Qualitative Inquiry: From "self and other" Binaries to the Poststructural Feminist Perspective of Subjectivity. *The Qualitative Report, 17*(47), 1-17. https://doi.org/10.46743/2160-3715/2012.1705

WordPress. (n.a.). Narrative Analysis. https://pluralisticpsych.wordpress.com/narrative-analysis/

Appendix A: Letter of Invitation

Greetings,

I hope this note finds you well.

I am currently a student at Walden University in the PhD program, working on my Dissertation Research Study. This research study will discuss national security, privacy and mobile forensics examinations. I am currently looking for volunteers willing to be interviewed who have at least one (1) year of experience as a Mobile Forensic Examiner. Participation in this study will be completely voluntarily.

This will include completing an Informed Consent statement (I'll e-mail this to you); and allowing me to interview you by phone, zoom or in person. The whole interview should take no more than 90 minutes of your time.

Please let me know if you would like to participate. Please let me know if you might be interested in participating and I will send you out the consent form which includes the full details about the study. I attend to start this process by 10/28/2020 and finish all interviews by 11/15/2020.

You can contact me by phone 224-627-8474, and/or e-mail charlesa.young@waldenu.edu if you have any questions.

v/r

Charlesa Young

Appendix B: Interview Questions

1. Are you familiar with the 2016 Supreme Court case Apple v. FBI?
2. With the FBI dropping the case, what is your take on tech companies helping or not helping law enforcement in such cases?
3. Do you believe that tech companies encryption methods, hinder mobile forensic investigations?
4. What are your thoughts when considering law enforcement conducting mobile forensic examinations concerning encrypted smartphones?
5. In your opinion, do you believe that if tech companies were to help during investigations, it would be a privacy concern for the public?
6. Regarding social media and privacy, do you think as individuals we give our own privacy away?
7. Do you think national security and privacy can collide with each other?
8. Are you familiar with the verbiage used within the 4th amendment? If so, can you explain what it means to you?
9. With the 4th amendment protecting individuals from unreasonable search and seizures, what are your thoughts when it comes to individual's personal media equipment?
10. What is your opinion regarding the forensic tool GrayKey only being available to law enforcement?

11. What is your overall opinion regarding a solution for the issues the FBI and Apple continues to face with each other? Should the courts step in or should law enforcement and technology companies figure out a solution on their own?