DRONES: DISCOVERING PERCEPTIONS OF AN INVASION OF PRIVACY IN RESIDENTIAL AREAS

by

Sandra A. Wright

A Dissertation Presented in Partial Fulfillment

of the Requirements for the Degree

Doctor of Science in Cybersecurity

CAPITOL TECHNOLOGY UNIVERSITY

December 5, 2016

DRONES: DISCOVERING PERCEPTIONS OF AN INVASION OF PRIVACY IN RESIDENTIAL AREAS

by

Sandra A. Wright

December 5, 2016

Approved:

Curtis R. Fox, D.Sc. Chair/Mentor

Ebonése Olfus, D.Sc. Committee

Michael R. Fain, Ph.D. Committee

Accepted and Signed: ____________________ 5 Dec 2016
Dr. Curtis Fox — Date

Accepted and Signed: ____________________ 5 Dec 2016
Dr. Ebonése Olfus — Date

Accepted and Signed: Michael R Fain 5 Dec 2016
Dr. Michael Fain — Date

Director, Doctoral Programs
Michael R. Fain for Helen G Barker 5 Dec 2016
Helen G. Barker, DM — Date
Dean of Academics
Capitol Technology University

ABSTRACT

Private residential users purchase and deploy cyber devices in their daily lives throughout their homes. The specific problem studied in this research was of residents' lack of understanding the laws and regulations regarding the right to privacy regarding drones, which could be used to violate those privacy rights. The purpose of this qualitative phenomenological study was to understand how private citizens perceived privacy when drones flown over their residences could access cyber devices operating within their homes. Four major themes which materialized from analytical data drawn from respondents surveyed in a Linthicum Heights, Maryland neighborhood, were: (a) cybersecurity practices; (b) laws, policies, law enforcement, fines, notifications, and reporting; (c) residential education in cybersecurity; and (d) package deliveries by drones. Findings revealed respondents' perceptions included a high desire for better cybersecurity training, laws to protect residences, their cyber devices, and their information, and the opportunity to benefit from technological advances in drone capabilities to deliver packages to residential areas.

DEDICATION

I dedicate this work to those who have been there for me night and day, in good times and bad throughout this entire effort; first to God, to Christ my Lord and Savior, and then to my husband Sherman, my daughter Andrea, my son Sherman II and his wife Jontay, my mother Jannie, my mother-in-law Margie, my sisters Glennette, Charlene, and Sylvia, to my brothers Charlie “Butch”, Arthur, Roger, and Derek, my cousin, Michael, and to my niece Shonne.

ACKNOWLEDGEMENTS

Many family and friends were anchors at pivotal points in this study, such as best of friends, Bonnie, Cynthia, Deborah, Deirdre, Ellen, Janet, Kris, Liz, and Telia. There are just so many people I would like to thank who influenced my studies and pushed me when I felt the goings had gotten too rough, but time and space are limited; however, they know who they are and I thank each one. Although not representing views of any U.S. Government entity, this work of art could not have been accomplished without our higher education financial support system or the many professors and cohorts who provided valuable instruction and advice, mainly because I needed it.

From Dr. Helen Barker, who energized me from inception and throughout, to my early advisor, Dr. Jason Pittman, to Dr. Michael Fain who encouraged continuance, to my chair and mentor, Dr. Curtis Fox, who shared similar concerns, saw my work's worthiness, and provided valuable guidance throughout this research. Special thanks to my committee members Dr. Char Sample and Dr. Ebonése Olfus, both knowing intensely of my passion for this subject and who have been with me from the start, remaining extremely key up to the final leg of this journey. With countless hours on bended knees in prayer, hope, and encouragement, I think this best sum it all:

> They disciplined us for a little while as they thought best; but God disciplines us for our good, in order that we may share in his holiness. No discipline seems pleasant at the time, but painful. Later on, however, it produces a harvest of righteousness and peace for those who have been trained by it. Therefore, strengthen your feeble arms and weak knees.
>
> Hebrews 12:10-12 (New International Version)

TABLE OF CONTENTS

List of Tables

List of Figures

CHAPTER 1: INTRODUCTION

Challenged with an abundance of drones being sold, Anderson (2013) noted privacy concerns were raised due to the number of drones seen flying throughout residential areas. Harrington (2015) made an observation of regulatory laws and privacy rights lag behind technological developments, which address drones capable of being used to invade a person's privacy, in unconstitutional searches, or in some cases used by private citizens to make people feel insecure in their homes. According to Jacobstein (2013), data can be collected using drones and shared in the cloud without a person's consent making this capability an even greater threat to violating a person's right to privacy.

The Fourth Amendment (1791) of the U.S. Constitution's Bill of Rights asserts people have the right to be secure within themselves, their homes, and their belongings, being free from unreasonable searches; and as stated by Nagy (2014), the public has "a reasonable expectation of privacy" (p. 148). Choi-Fitzpatrick (2014) identified drones as unmanned aerial systems (UAS) or vehicles (UAV) subject to privacy infringements. According to Peppet (2014), drones are considered big data devices either lacking or associated with weak privacy policies.

Chapter one presents a brief description of the background of privacy policies and drones, privacy issues with drones in residential areas, and the purpose of this study. The significance section highlights the uniqueness of the approach, provides an overview of those who may benefit from the results of the research, and adds to the overall body of knowledge. The nature of the study section includes an overview of the research design proposal and method appropriateness, and addresses several research questions. The goal of this qualitative phenomenological study was to recognize and discover residents' perception of drones flown in their reasonably expected private living areas.

Background of the Problem

The Fourth Amendment (1791) forms one of the basic premises for people to be secure in the privacy of their homes, free from unreasonable searches, and extends certain rights affecting activities in personal settings and adjacent airspaces. Dolan and Thompson (2013) stated drone policies were put into place by federal organizations to permit drones to operate in U.S. airspaces through appropriate regulations. However, Pomeroy (2015) noted the urgency to establish parameters for drones that rapidly populate airspaces, which has led to different aspects of what constitutes the right to privacy and where those rights are extended. Brandeis and Warren (1890) indicated rights would have to be defined and further redefined based on various situations in personal and property protection, as well as societal ramifications in growing demands of tangible and intangible possessions.

According to Jacobstein (2013), drones are indicative of associated loss of privacy and lacks regulatory direction, so operators, residents, and those taking part in flying drones may not know the confines to operate a drone within residential areas. According to Ahn, Bang, and Lee (2011), being aware of circumstances is beneficial in taking appropriate steps to protect one’s privacy based on federal laws and regulations. The phenomenon of drones circulating around private living areas poses the risk of security infringement through an invasion of privacy and unauthorized data sharing through cloud computing (Jacobstein, 2013). Arapinis, Bursuc, and Ryan (2013) observed concerns for privacy in cloud computing, which is a type of service provided remotely by an external party.

According to Dolan and Thompson (2013), Federal Aviation Authorities’ (FAA) regulate drones through the Federal Modernization and Reform Act of 2012 (FRMA), which dictates the use of national airspace for UAS’ (a.k.a. drones). Some airspace parameters have been set restricting drone flights to 400 feet and below (Mack, 2014); however, there are notable privacy challenges. Security apprehensions of midair surveillance were noted in a Congressional Research Service (CRS) report where invasion of privacy was implicated from visual data collection and recording of people from drones (CRS, 2015). As cases continue to evolve, handling of these complaints vary from state to state as seen in California and Florida where a number of privacy complaints were made regarding drone sightings. Due to the lack of Maryland policies on drones and privacy, Maryland was not used as an example.

According to Choi-Fitzpatrick (2014), California established legal boundaries affording privacy on private property and prohibiting wandering eyes through drone cameras. Villasenor (2013) shared deep concerns if the government attained a warrant and exercised unrestrained rights to access, collect, and view descriptive images of a household, these images may reveal persons unclothed. Villasenor (2013) also indicated worries an invasion of privacy or other unauthorized act was possible when domiciliary images were captured from a UAS. For example, nude photos acquired could lead to further exploitation and could be distributed through the cloud. Mack (2014) suggests UAVs, such as the MQ-9 Reaper, have the capability to detect heat measurements of a person’s body from an alarming 37 miles away, so what is expected to be private may be captured by a drone hovering in airspaces outside.

In Florida, a woman found a disabled drone lying upside down on her lawn in September 2015 (Anonymous, personal communication, September 12, 2015). The victim reported the incident to the police department and questioned the drone’s ownership, what data was collected about her and her home, and she wanted to know about her rights and the laws governing the situation. The woman felt her rights were violated; however, the local police department only took possession of the drone and classified the incident as a lost and found without providing any satisfactory answers (Anonymous, personal communication, September 12, 2015). There were two occasions where a drone was sighted flying over private residences in a Linthicum Heights, Maryland neighborhood; however, no police activity was seen and it was not known if any reports were filed by any of the residents (Anonymous, personal communication, June 19, 2016 & July 4, 2016).

In another situation, Tampa police responded to an incident in which a man was flying a drone on his own property and was approached by a neighbor who was in possession of a firearm (Billi, 2015). According to Billi (2015), the drone owner was seen flying his drone throughout the neighborhood earlier in the day, but the reporting officer only asked questions about the alleged invasion of privacy, stated more research was needed, and left with no actions taken. Whether a government agency or private citizen is involved, Thompson (2015) indicated privacy concepts are continuously analyzed as legal rules of surveillance and privacy rights become ambiguous in public and private drone operations. Barocas and Nissenbaum (2014) described privacy issues against Big Data where actions on data collected inferred revealing personally identifiable information, such as name, address, or social security number.

Big Data denotes the technological challenge in the proficient handling of traditional data conventions in new architectures based on characteristics of volume, variety, velocity, and variability (National Institute of Standards and Technology (NIST) Special Publication (SP) 1500-1, 2015). A drone could be capable of conceptually collecting Big Data when associated with other related or dissimilar data could provide new details about the unprecedented bit of data; thus, according to Peppet (2014), such details could unexpectedly infer revelations of a person’s lifestyles, tendencies, and behaviors. McBride and Stough (2014) identified big data as being made up of number sets that could be contextualized and further translated into useable information; thus, vital information could be revealed through such translation. As illustrated by the authors, the number *one* could notionally be transformed into an action taken by land; whereas the number *two could* translate to an action taken by sea (McBride & Stough, 2014). Deducing these kinds of translations could be problematic by revealing vital information throughout various situations.

Problem Statement

The general problem is as thousands of drones are sold for recreational purposes, some are being manipulated into areas where unlawful viewing and data collection of a person's private area can occur (Choi-Fitzpatrick, 2014). The ability to use smart phones and other new technology to control drones have made UAS' lucrative to operators, in part because of the low purchase cost to acquire them and because of the device's adaptability (Mills, 2015). A UAS hovering over a person's private property jeopardizes personal privacy and can contribute to further unauthorized data sharing in the cloud (Jacobstein, 2013).

The specific problem is residents lack understanding of the laws and regulations regarding the right to privacy regarding drones, which could be used to violate those privacy rights. There are federal laws regulating drones used in commercial areas, such as airports (FAA Modernization and Reform Act of 2012). However, residents may not be educated about vulnerabilities associated with data collection gained from drones that could lead to inappropriate data sharing of personal information (Jacobstein, 2013). Further, a resident's perception of drones operating in their private areas may identify a lack of understanding of their right to privacy or what constitutes an invasion of privacy. Pomeroy (2015) indicated with the complexity of drones integrated in airspace, residential awareness of privacy laws and property rights are needed in promoting legislative measures.

Although separate phenomenons were found to have occurred in Florida and Maryland, it was more advantageous to focus the research on Maryland. The general population for this study involved a small Linthicum Heights, Maryland neighborhood, where only one adult was expected to participate from each of the selected households. Creswell (2012) suggested information be collected on the study population to capture participant characteristics for possible use in surveys. Thus, narrative discussions were used to summarize findings of the analyses based on the phenomenon addressed by a handful of residents' perceptions of their invasion of privacy experiences.

Purpose of the Study

The purpose of this qualitative phenomenological research was to understand how private citizens perceived privacy when drones flown over their residences could access cyber devices operating within their homes. Qualitative research allowed exploration of a study through interviews where opportunities exist for immediate clarifications that attributed to phenomenological insights gained from individual experiences (Akkoyunlu & Daghan, 2014). Salkind (2012) stated qualitative research best serves to describe exploratory processes through interviews, which depict the narrative design as an appropriate tool for performing this research. Salkind (2012) also indicated a narrative design was consistent with qualitative phenomenological research through examinations in social, cultural, or political context gained from participants' experiences.

The objective of this study was to identify what residents perceived about their privacy rights, to understand what they believe constitutes an invasion of privacy, and to provide information that allows residents to become more knowledgeable about drones flown over their residences. Information was gained through interviews of personal accounts and provided the opportunity to capture educational needs in privacy protection. Interviews were an added value to open-ended web-based survey questions that addressed participant experiences over one or more situations with drones. Finfgeld-Connett and Johnson (2012) indicated qualitative research mostly supports contextual issues in a given situation to better identify the problem; therefore, qualitative research was most fitting for this research.

The geographic location of this study was a small Linthicum Heights, Maryland residential neighborhood targeting 18 residences. Only one adult from each household was sought to participate as an interviewee and although the possibility existed that the study could have extended to other individuals, sufficient information was captured from each participant. Englander (2012) shared subjectivity of another is key to phenomenological researchers seeking descriptive collection and discovery of information towards understanding the phenomenon. The intent of this qualitative phenomenological approach was to avoid falling into pitfalls of blurring collective details as Applebaum (2012) proposed has happened with various qualitative researchers.

Significance of the Study

A significant amount of literature and laws already exists for privacy rights. Because of rapid advancements in drone technology and ease of accessibility, drones are a big hit to the public today as were personal computers decades ago (Anderson, 2013). This revelation netted new privacy concerns and prompted the exploration of the phenomena through this study. Whether drones are used for legal surveillance or recreational purposes, privacy laws require knowledge and understanding enabling proactive protective measures to privacy (Ahn, Bang, & Lee, 2011). Thompson (2015) indicated privacy laws governing drones used in private areas appear to be lacking or are inconsistent across the United States, to include varying states' interpretation of reasonably expected privacy.

A 2014 executive report to President Barack Obama noted the makeup of policies and laws on new technological advancements were not understood by the American public (Gray literature, 2014). Consequently, new developmental changes brings an increasing need for updates to privacy policies, laws, and educational awareness, especially for drones where laws may minimize risks; yet, restrictions may deprive the benefits of operating drones (Jacobstein, 2013). According to Terwilliger (2013) and Jones (2014), higher education and communication is key to innovative studies, such as this research on privacy issues with drones. Therefore, results of this study may yield tremendous benefits and contribute to the field of study for scholars, policy makers, law enforcement, residents, and even convicts in identifying deficiencies in education and privacy laws.

Redefined laws could be established on residential privacy rights to include adding fines and retributions for illegal surveillance, invasion of privacy, or other violations in drone use. For instance, Miller (2015) stated police authorities could use drone technology to gain sensory information, such as visual recordings on a suspect's movement by going through Global Positioning System (GPS) tracking. In these instances, individuals with law enforcement tracking devices (physically attached electrical surveillance devices) may feel they are being unfairly spied upon when drones are operated over private areas; Pomeroy (2015) concluded drone surveillance in such cases was a violation of one's rights. Miller (2015) indicated another significant matter on tracking where it is a violation of the Fourth Amendment to track a person without a warrant or in cases of unreasonable searches.

The outcome of this study was formalized from the results of personal interviews and online surveys of participants' personal experiences with drones. Thus, the analyses are reflective of information collected through narrative discussions. Material presented up to this point discusses the significance of this research in personal and legal situations leading to the next section, the nature of the study, which presents a review of the research methodology.

Nature of the Study

According to Erkip and Mugan (2010), qualitative research is the most appropriate approach to use when gaps exist in the literature surrounding the subject. The authors noted an advantage to qualitative research was to discover experiences of each participant and allow recollection of others who were involved in the phenomenon (Erkip & Mugan, 2010). A qualitative phenomenological approach was best suited for this study over other research designs because it identified with participants' lives, the participants' perceived thoughts, and implications recognized because of the phenomenon as implicated by Akkoyunlu and Daghan (2014). This study was performed in a small Linthicum Heights, Maryland neighborhood where recommendations materialized from participant perceptions that could improve privacy awareness of drones operating in residential areas. To better understand the makeup of this research, the nature of the study was presented in a discussion of the research method appropriateness and research design appropriateness.

Overview of the Research Method

A qualitative phenomenological method allowed the gathering of information on adult residential citizens regarding their perceived expectations of privacy related to drones. Erkip and Mugan (2010) indicated a qualitative research approach was most appropriate when gaps exist in the literature surrounding a study. This qualitative research was structured in a fashion that acknowledged the exploration of the study through interviews, clarifications, and document examinations attributed to the phenomenological insights gained from individual experiences (Akkoyunlu & Daghan, 2014).

Suggested by Erkip and Mugan (2010), there are advantages to performing a qualitative research in the discovery of participants' experiences when a particular event happened. According to the authors, a 1999 Haraldsen article stated qualitative research was more successful when used in small neighborhoods (Erkip & Mugan, 2010); thus, this approach was most suitable for querying the small Linthicum Heights, Maryland neighborhood where 18 adults were sought for interviews. While qualitative methods sufficed for this research, other research methods had advantageous characteristics to support different approaches and populations.

Licqurish and Seibold (2011) noted grounded theory design supported research processes and situational commonality, examinations of certain similar theoretical perspectives, and the social interactions of individuals. Goldman, Kitto, Peller, and Reeves (2013) noted although ethnographic qualitative designs offered identification of linked social phenomena, ethnography was difficult to perform, analyze, and understand due to embedded discourses. Experimental design was also not selected since researchers perform quantitative studies using more than one group of participants where validation of threats to the study results were controlled, eliminated, or minimized (Haegele & Hodge, 2015).

Overview of Design Appropriateness

The purpose of this qualitative phenomenological study was to bring to the forefront the experiences and feelings of participants' experiences of privacy violations regarding private, individual drone activity around a Maryland residential area (Anonymous, personal communication, June 19 & July 4, 2016). Qualitative narrative designs allow data collections, analyses, and reporting through the descriptive retelling of participants' experiences of central phenomena (Creswell, 2012). Harding et al. (2015) presented a qualitative pictorial narrative research derived from study data through a textual research undertaking. Colyar and Holley (2012) emphasized researcher commitments to writing qualitative narratives were found successful through interpretative stories and then those stories shared with a broader audience. Therefore, the addition of non-textual material increased understandability that supported collaboration gained from a participant's story of the phenomenon as denoted by Harding et al. (2015).

Other designs were analyzed, but proved inappropriate for use in this study: hypotheses were found favorable in quantitative researches; theories required testing; multiple variables needed to be measured; comparisons and differences required association between groups; and closed-ended questions led to deductive researches (Creswell & Plano Clark, 2012). Reviews of mixed methods showed unsuitability to handle problems this study focused on since mixed methods are based on theoretical assumptions and generalized exploratory findings (Creswell & Plano Clark, 2012). Therefore, a qualitative design proved most beneficial due to the study's narrative characteristics.

According to Creswell (2012), qualitative narrative designs allow an understanding of individual experiences gained through personal and chronologically presented details, oral recounts in the retelling of stories segmented by themes, and with minimum use of literature. Following along with Creswell (2012), the researcher was noted as the inquirer while the participant was actively involved as the story developed through detailed descriptions of settings associated with the phenomenon. Also, personal interviews gave the researcher opportunities to hear unadulterated and quality recounts through narrative research designs recorded and transcribed with confidentiality, as suggested by Cassell and Symon (2011).

Research Questions

Suggested by Akkoyunlu and Daghan (2014), the goal of empirical research questioning is to gain knowledge of what was experienced and to identify the nature of the situation that had a bearing on those experiences with the phenomenon. The research design allows experiences to be drawn out from first-hand knowledge and to identify what is known to be legal, understood, misinterpreted, or disregarded (Wolper, 2012). According to Cone and Foster (2006), research takes on a more in-depth state of questioning to show an understanding of what exactly will be studied once the general question is formed and then the study smoothly advances.

According to Conrad, Lind, Reichert, and Schober (2013), electronic questions exacts real instinctive responses from participants who are more apt to share information when questions are provided electronically. Three fundamental questions were at the forefront of the interviews assisted in the composition of the electronic questionnaire:

1. How did residents feel if faced with a drone flying within their residential private spaces and accessing their cyber devices?
2. How did residents feel about drones entering their private spaces, collecting data about them, and placing that data in a cloud?
3. How did residents feel regarding law enforcement’s handling of drones flown in residential areas?

Question 1 addressed how residents felt they would react if faced with a drone flying over their private living areas and accessing their cyber-enabled devices. Florida law was used due to the lack of applicable Maryland policies on drones and privacy. As noted in Florida’s

Freedom from Unwarranted Surveillance Act (FUSA) (2015), it is illegal to perform surveillance without written consent as it violates the person's reasonably expected privacy. These rights are further extended to ground level observations whether a drone is used or not (FUSA, 2015). As of this writing and despite at least two attempts, Maryland does not have any laws governing drone operations. Maryland House Bill 875 was up for consideration to address surveillance, illegal information gathering, and law enforcement's use of drones in evidence gathering, however, the bill was later deemed dead (Maryland House, 785). Then House Bill 351 would have at least addressed criminal procedures in Government drone use, but that bill was withdrawn in February 2016 (Maryland House, 351).

Question 2 addressed participants' feelings when drones could be used to gain personal information without permission when flown over their private residences. Although a forerunner to privacy rights, the Privacy Act of 1974 could be used to allow the collection of relevant information through authorized drones, but Nagy (2014) indicated the public has "a reasonable expectation of privacy" (p. 148). Reynolds (1978) discussed expectations of privacy as people have the right to feel secure in and around their homes and that they are to be protected from unreasonable searches or the search and seizure of their things without cause.

Question 3 addressed educational awareness in the legal use and handling of drones found operating within residential areas. Private citizens' awareness of actions they can take according to laws on drones flown over residential areas may help increase personal privacy awareness and protection. According to Florida's Freedom from Unwarranted Surveillance Act, people, organizations, nor any governmental sector is permitted to use drones with recording capabilities to take still pictures or record a property owner, their property, or anyone occupying the property, not even the resident's guests (FUSA, 2015).

There were three areas of concentration related to each of the research questions. One area captured information regarding the central phenomenon of participants' perceived drone experiences. Another area focused on participants' awareness of drone capabilities to gather information. The third area examined information on legal actions in the handling of drone situations within residential areas. Querying participants on these three distinct areas allowed additional exploratory questions to be formed and participant responses to be based on what each person believed a situation meant to them, comparable to Applebaum (2012).

Conceptual Framework

Green (2014) made the stipulation theoretical and conceptual frameworks were not generally designed into a research method. The framework for this study, however, was built on three research questions and several qualitative narrative research characteristics as identified by Creswell (2012). This approach guided and formed an organized structure for the study and provided assurance the study was performed in a coherent manner, as discussed by Green (2014). This section discussed relevant details on key matters, viewpoints, and discourses on privacy rights; however, Maryland law was not referenced due to the lack of applicable Maryland policies on drones and privacy; therefore, Florida law was used.

The Privacy Act of 1974 set the stage for this study, which took into consideration the public's reasonable privacy expectations (Nagy, 2014). A forerunner to privacy rights, the Privacy Act allowed the collection of relevant information; whereas Reynolds (1978) discussed expectations of privacy in cases of search and seizure in relation to the Fourth Amendment. According to Demchak and Fenstermacher (2009), Section 934.50, Florida Statutes (2015) was the initiative mandating law enforcement acquires a search warrant when drone-use was needed to perform evidence collection; Section 934.50 is Florida's Freedom from Unwarranted

Surveillance Act (FUSA). Even in the midst of drones circulating throughout residential neighborhoods, Molko (2013) noted the Fourth Amendment provided protection from unreasonable government invasions. The author further indicated the Supreme Court was faced with legal concerns of drone surveillance performed in private settings by law agencies were involved in theft and drug investigations (Molko, 2013).

According to Molko (2013), there will be a reduction in privacy when the predicted 30,000 drones become operational around 2020. This study showed the correlation of perceived privacy rights in residential situations when drones were operated in reasonably expected private areas, whether the drone was operated by a government entity or not. Numerous privacy rights have been studied where drones were used to uncover or assist in legal matters, as with the hunt for the Washington sniper (Bewley-Taylor, 2005). In Paust's (2015) examination of privacy rights, a reformation of human rights protection was warranted if the public's expectation of privacy was not considered. These situations implied some level of knowledge of applicable privacy laws and policies were understood, particularly when dealing with drones in this study.

Definitions

The following terms as defined were used throughout this study that enhanced understandability in a contextual manner.

Big Data. A term used to describe a vast amount of data available throughout network topologies using electronic or digital means where information is continuously sought; big data is characterized by volume, variety, velocity, and variability (NIST, 2015).

Cloud. A term used to indicate the existence of a group of computer systems, devices, and connections to support cloud computing (Merriam-Webster, n.d.).

Cloud computing. NIST defined cloud computing as a cloud model that allows extremely fast on-demand access to globally shared computing assets that can be quickly established with little management by service providers (NIST, 2015).

Denial-of-service (DoS). One or more actions to preclude any portion of an information system or device from operating (CNSSI 4009, 2015).

Distributed DoS (DDoS). Use of various devices or hosts to execute a DoS attack (NIST, 2013).

Drone. "An unmanned aircraft or ship guided by remote control or onboard computers" (Merriam-Webster, n.d., drone).

Internet of Things (IoT). Reference to a device or object capable of automatically transmitting and/or receiving data over the Internet (Department of Homeland Security (DHS), n.d.).

Navigable airspace. The airspace used for appropriate flight operations at or above authorized altitudes (Aeronautics and Space, 2015).

Ransomware. "A type of malicious software, or malware, designed to block access to a computer system until a ransom is paid. Ransomware is typically spread through phishing emails or by unknowingly visiting an infected website" (DHS, n.d., malware).

Surveillance. The viewing of private residences and their owners, occupiers, dwellers, visitors, or lessees with enough detail that clearly reveal intricate information on those persons, their identities, practices, behaviors, activities, or locations; or, the scrutinized viewing of private property by pinpointing the distinctive material enhancements of the property or of its occupants (FUSA, 2015).

Unmanned Aerial System (UAS). Complete communication links and constructs of an unmanned aircraft vital for safe and efficient operations in national aeronautical systems (FAA Modernization and Reform Act of 2012).

Voyeurism. According to South Carolina Code of Laws (2001), voyeurism is a purposeful act to satisfy a voluptuous need through peeping, photography, audio and video recordings, or digital data creations, to include the sale or distribution of such information of another individual without their knowledge or permission (16-17-470).

Assumptions

According to Haegele and Hodge (2015), an understanding of basic assumptions in a study allows research to be critically conducted, analyzed, and presented in a stellar fashion. Snelgrove (2014) noted there is a phenomenological importance of inquiries of a person's conscious perception of situational views. There were three all-encompassing assumptions under consideration for this qualitative phenomenological study. First, there was the assumption participants would be honest and without deception. Second, an assumption existed participants would be willing to provide open and complete comments of their feelings based on interpretation of their perceived drone experiences. Finally, participant responses would be without influence. Aluwihare-Samaranayake (2012) suggested consideration of respect and justice within the representative experiences of participants were through reflective questioning.

Based on collaboration that took place between the researcher and the Maryland participants, research questions were the focus of the dialogue of this phenomenological study. Through a chronological and contextual manner, focus was on quality narratives captured into themes as a reflection of each participant's perception of their experience with drones. The following is a discussion on the scope, limitations, and delimitations regarding the data used during this study.

Scope, Limitations, and Delimitations

According to Finfgeld-Connett and Johnson (2012), saturation of data collection is when there is complete explanation between conceptual views attained from perceptive and arduous combing of research information. The authors noted not having enough studies available has an effect on saturated findings (Finfgeld-Connett & Johnson, 2012); however, Knapik (2006) completed a qualitative research using 90-minutes of recorded interviews collected from only four participants. Saturation was reached in this study when enough information was gained regarding the research questions, which were posed to 14 adult participants of the 18 households sought. This phenomenological study helped identify residents' perceptions of privacy when drones were flown in their reasonably expected private living areas.

Scope

This research addressed the main research question, "what perceived privacy rights are associated with private, individual use of drones operated in a Maryland residential area?" A survey, which was presented to 14 respondents of the 18 targeted residences, identified the participants' knowledge level of their perceived privacy rights in drone operations, whether the drone was operated by a government entity, another party, or even by the participant. Applebaum (2012) noted qualitative research resulted in inter-related findings between participants, so posing the same questionnaire allowed the study to stay centrally focused within a controllable level and permitted further questions and discussions to evolve between researcher and participants.

Limitations

Lack of knowledge, or understanding of what constitutes reasonable expectation of privacy and the ability to grasp the severity of invasion of privacy occurrences through use of drones could impact intelligible survey responses. The educational level of proposed participants was not readily known and required different levels of discussions on the same material between participants as each interview took place. For instance, a participant may not have known what a drone looked like and therefore, would not have known what vulnerabilities or risks were at stake concerning their perceived right to privacy. According to Knapik (2006), it may be necessary for researchers to adjust their interactive approach based on participants' academic levels.

Time constraints drove the level of discussion between the researcher and participants, but as noted by Cassell and Symon (2011), there was no need to expend additional time during the qualitative research because of difficulties to seek alternative criteria. Creswell (2012) expressed limitations were merely hypothetical disadvantages realized by researchers and results may have become affected based on those limits and shortcomings. It was expected other limitations would be realized during the actual performance of this study would cause considerations be made from delimitations. Additionally, lack of applicable Maryland laws and the lack of availability of the initial Florida resident who experienced a drone sighting in 2015, resulted in research limitations. Consequently, the geographical location was changed from Florida to a Maryland neighborhood with reference to Florida law due to the lack of Maryland policies on drones and privacy.

Delimitations

Limitations require adjustments because of how a study is going due to the importance of certain positions, such as when Wahlstrom (2008) realized listeners were subject to being manipulated. Recent drone sightings over an Anne Arundel County Maryland neighborhood (Anonymous, personal communication, June 19, 2016; July 4, 2016) changed the study venue from Florida to Maryland; however, Florida law was referenced due to the lack of applicable Maryland policies on drones and privacy. The study was performed in Linthicum Heights, Maryland a neighborhood where approximately 18 adult residents experienced the same drone events on Father’s Day and on the 4th of July 2016.

This study did not include children and was limited to adults with a fair understanding of drones so unadulterated data could be obtained from informed participants. The researcher did not discuss or take part in discussions with neighbors on the drone sightings and avoided perpetrating biases. Decisions affecting these and other situations were addressed as challenges surfaced once the study was underway. Therefore, information and decisions, such as the venue change, was captured to afford repeatability and feasibility decisions by subsequent researchers.

Summary

Chapter 1 presented overviews of privacy policies and problems with drones being flown in areas affecting private residences. A brief look was provided on the importance of how and what drone capabilities can affect perceived expectations of privacy (Nagy, 2010). Lastly, the introduction of the qualitative research also provided a review of the research design and research questions were included for use as a guide to the study.

Descriptive terminology was included to aid in material understanding and to avoid ambiguous meanings or misconceptions when the study was performed. The scope identified specifics on the number of participants targeted and where those individuals resided who were likely candidates for the study. Assumptions and limitations surfaced during the research were discussed, as well as delimitations that further materialized when the study was underway.

Chapter 2 provides the literature review through title searches, article reviews, as well as reviews for document and journal researches. A historical overview covers literature gaps, current findings and studies, and research variables as they relate to research questions throughout the literature review. Chapter 2 concludes with a balanced discussion to compare and contrast various viewpoints regarding research in the right to privacy, especially as it relates to drones flown over private residential areas.

CHAPTER 2: REVIEW OF THE LITERATURE

The purpose of this qualitative phenomenological research was to understand how private citizens perceive privacy when drones flown over their residences have the capability to access cyber devices operating within their homes. Experiences with drones could be derived from first or second hands-on knowledge of drones with or without options, such as built-in or externally mounted cameras or video functions. Anderson et al. (2016) demonstrated a camera or some version of a video recorder could be integrated into a drone or externally mounted; proving recording capabilities were successful merely with an android-based phone mounted to a drone. In another case, the authors exhibited recording using a makeshift platform and an android-based phone mounted to a kite (Anderson et al., 2016). Capturing participants' perception of drones and their capabilities significantly contributed to the success of this study, as well as completing an expansive literature review.

An examination of a number of references were used to ascertain the originality of the aforementioned material and those that followed, sort of a finding out who researched it first concept as noted by Creswell (2012). There was an anticipation of difficulty locating primary sources of original research studies for new technology, so the literature review consisted of online searches for peer-reviewed material through Capitol Technology University's (CTU) Virtual Library and other trustworthy sources. The CTU library offered access to a tremendous number of online books, journals, dissertations, and electronic literary sources, particularly the Academic Search Premier tool, EBSCOhost, a copyright of EBSCO Industries. EBSCOhost provided diverse computer search indexing and database search functions; additionally, SAGE Publications, Educational Resource Information Center (ERIC), and ProQuest® offered easy data retrievals via CTU's Virtual Library.

Chapter 2 provides literature reviews on material used to gain or expand knowledge based on the characteristics of drones, drone governance, and cybersecurity awareness. It showcases certain capabilities and characteristics of a typical private drone identified through title searches, articles, research documents, and journals. Creswell (2012) noted encyclopedias can be referred to when unfamiliar with the functionality of terms; dictionaries to support comprehensive increase in knowledge on key terminologies regarding new-age technology; and handbooks could be used because of their specialized functions, mediums, and common reviews.

Categorization of key terms was used to narrow references for selection and evaluation, backed by constructive decisions based on note-taking, diagrams, charts, and tables, to help in the summation of the selected material as proposed by Creswell (2012). Key words, such as Big Data, drones, perception, privacy, UAS, and UAV were used to draw major articles through queries. While terms UAS, UAV, and drones were introduced in Chapter 1, they were frequently used interchangeably; therefore, reference in this literature review primarily reflected the terms as used by the authors under review or as attained from educational portals, collaboration areas, and source material. The information discovered complemented a historical overview, provided insight to current findings, and presented a balanced discussion of alternative viewpoints from varying authors.

Title Searches, Articles, Research Documents, and Journals Researched

Creswell (2012) noted it is beneficial to identify specific search terminology amongst the massive amount of available data to discover substantial supporting material for research. Denning and Frailey (2011) organized a set of professional terms in a table to capture related professions and activities during their study of information technology. For this writing, the word list in Appendix A was used to begin the search of relative qualitative study information through a plethora of means, title searches, articles, research documents, and journals.

Material was examined for applicability, scrutinized, and then discussed within the literature reviews. Although drones have existed for a while, drone functionalities and the way people perceive drones were examined through historical overviews. Dialogues of current findings followed in order to present the ever-changing technology and new interfaces constantly introduced with drones.

Title Searches

Title searches over the Internet were used to find data on drones with and without built-in cameras or recorders, regarding privacy sources, and to extract historical information from key search arteries, such as electronic databases, libraries, and other archives. Since countless titles were available, a look over different periods assisted in the compilation and narrowing of selections, beginning with historical information and attention paid to search terms in titles as suggested by Creswell (2012). Title searches performed periodically during the research through completion could allow the capture of new terminology and relevant, up-to-date information.

Articles

Creswell (2012) indicated articles could be used to exact different experiences, knowledge bases, and relevant information sources from users, developers, installers, and merely those who observe certain instances, such as the perception of an invasion of privacy. Articles were sought based on past and current trends of public demands seeking to obtain personal drones and a cursory review of conferences and venues was performed to include additional articles on this study topic. Harris (2013) noted opposition to an editorial policy change, so material presented during this literature review, which was intended to reflect varying differences, may be indicative of legal issues, or the material actually represented two or more shared views on a particular editorial discussion.

Research Documents

In some cases, electronic research documentation, hard copy reports, newspapers, or other physical artifacts were available. Therefore, one of the search criterions included peer-reviewed documents created or updated within the last five years from the date of this study. Creswell (2012) noted the use of ERIC to capitalize on nationally vested interests as a key information retrieval conduit, especially since ERIC was made possible for public consumption using public monies.

Journals Researched

Journals were important inputs into this research consortium that allowed the grasping of key information from national and international sources. Blalock and Gilchrest (2013) indicated certain areas for concern when using journals, such as the abundance of copyrighted material covered in journal articles or requiring the explicit acknowledgement of an author when a particular work was referenced. Care was used to ensure all sources were justly acknowledged and plagiarism avoided at all costs during the entirety of this writing, to include self-plagiarism. In following Chrousos, Gravnis, Kalantaridou, and Margioris' (2012) implied suggestion and as the author of this document, other work authored, published, and included in this literature review was duly referenced to avoid self-plagiarism.

Historical Overview

UAS', UAV's, and drones have been widely used in military and civilian operations, and dependent on actual use, regulated by national, federal, or local governance (Barry, 2013). Villasenor (2013) provided details on drones utilized in corporate and economic espionage that went beyond a perpetual 6300 military drones reported in-use in 2012. The growing civilian demand and domesticated uses led to the statutory needs of privacy protections governing UAS' (Villasenor, 2013).

According to Dolan and Thompson (2013), considerable amount of legal concerns prevailed in the 19th century where technology lagged behind societal changes and demands, in cases of trespassing, eavesdropping, and surveillance. Even so, the right to privacy Brandeis and Warren (1890) advocated in the 1800's went up against the task of defining just what privacy meant. Centuries later, privacy and what violates it are still being challenged in areas that could be construed as public, personal, or private. Choi-Fitzpatrick (2014) denoted closed-circuit television was the predecessor to UAVs in commercial monitoring of public areas, such as parks and recreational sites; he further noted the military deemed *remotely piloted aircraft* as the appropriate term of use regarding UAV, UAS, or drone. According to Choi-Fitzpatrick (2014), a common denominator in drone application, from inception to current uses, has the potential to jeopardize personal privacy.

Current Findings

Barry (2013) speculated the need for protection of privacy in the new technology age of drones and advocated democratic governance, which promotes appropriate drone use. During the literature review, details on personal privacy rights and governance discussions were highlighted on societal influences, such as noted by Barry (2013). Current findings and studies were presented based on different aspects and positions that began with typical characteristics of a drone while noting gaps found in the literature from era to era. Snelson (2016) noted there were existing literature gaps with new technology, such as social media, and use of trending qualitative research through interviews and other approaches (e.g. focus groups) supported gaining insight to the way people participated in activities based on their experiences. Explanations of drone characteristics revealed different viewpoints on areas requiring protection, like the peering through a bathroom window where viewing could be made from the ground or another location, as noted by Sanders (2015). Standing behind the 4th Amendment, Sanders (2015) spoke on voyeurism in Florida that involved lewd offenses in acts against those expecting privacy in areas like a bathroom. Florida law was referenced due to the lack of applicable Maryland policies on drones and privacy.

How do residents feel if faced with a drone flying within their residential private spaces and accessing their cyber devices? How do residents feel about drones entering their private spaces, collecting data about them, and placing that data in the cloud? How do residents feel regarding law enforcement's handling of drones flown in residential areas? These three questions were presented in Chapter 1 and were key driving factors to locating literature on the subject matter. Literature on perceptions of UAS', UAVs, or drones were reviewed on how someone viewed their own privacy or whether they were aware of legal ramifications that could have surfaced during the operation of a drone. McBride and Stough's (2014) stance seemed to be perceptions of privacy experiences could have been influenced by one's familiarity with Big Data and the notion guaranteed privacy may have been compromised through exploitation.

Perception of Privacy Experiences

How people perceived privacy and what they felt could have constituted an invasion of privacy differed from person to person and event-to-event. According to Garton, Robertson, G. White, and S. White (2012), limitations that separate neighbors via walls assert an expectation for others to not impose on someone's privacy, which neighbors should stay out of concerns of others, and to respect a person's private domain. Although the report was focused on privacy based on sexuality, it provided details on expectations of privacy in neighboring environments.

Several viewpoints were noted regarding individual perceptions of privacy and experiences in various situations (Costante, Hartog, & Petković, 2015; Hamari, Karvonen, Lampinen, Oulasvirta, & Suomalainen, 2014). Costante, Hartog, and Petković (2015) identified three levels of users' perceived trust in privacy against a particular system, application, process, or location. The low, medium, and high variations were discussed in the form of a model examining trust decisions based on perceived expectations of an event and how those factors impacted decisions during electronic interfaces (Costante et al., 2015).

Hamari, Karvonen, Lampinen, Oulasvirta, and Suomalainen (2014) discovered people's expectations were affected by not knowing what to expect, the feeling of uncertainty basically led to a feeling of harm, and that people would rather not deal with the possibility of threats. The authors' nine scenario-based surveillance tests showed the significance of subject interactions centered on a situation, individuality, and intent resulted in a range of privacy concerns; domestic video surveillance was the highest ranked privacy concern (Hamari et al., 2014). The transparency of intentions study also showed people had a great cause for concern when they were made aware of a perpetrator's intended action against them (Hamari et al., 2014).

Because of what happened in a neighborhood or how residences reacted or perceived they would react to an event varied because of the socioeconomic variations and influential differences in a community (Vilalta, 2012; Cross, Hamilton, & Ramsey, 2012). Vilalta (2012) noted fear factors prevailed whether a security system was in-use in a home or not and surrounded presumptions and misconceptions of the inability to take appropriate measures because of affordability. Regardless, a sense of fear was perceived in both cases (Vilalta, 2012).

Observation showed there were influences based on perception of what actions performed by one were observed and used by another (Cross et al., 2012); such behavior was taken into consideration during this research.

Rausch (2011) analyzed privacy rights using the highly acclaimed case of Roe v. Wade where the focus was on property, that of a woman's body. The author's investigation revealed a lack of positive rights, as well as, a lack of precise statutory verbiage to distinguish property rights and ownership (Rausch, 2011). Volokh (2014) described a thought-provoking view of how tort law diminished the value of privacy, which was described to have fallen second to safety. It was further stipulated privacy was deemed to some extent, inconclusive and required passable delineation and fortification (Rausch, 2011). Similarly, Crowsey, Kar, and Zale (2013) shared their views on tort law, the inadequacies of privacy protection, and ubiquity of location reporting, surveillance, constant observation, and tracking, which were traditionally infringed upon through physical intrusion mechanisms.

Drone Capabilities and Characteristics

UAV operators have noted many reasons why unmanned aerial systems were making their way through urban territories. Brouwer et al. (2015) praised highly the camera characteristics fashioned on the up and coming popular drones because of their viewing and image captures used in environmental surveys; the camera's lightweight and wide-area lens capabilities allowed drones to be operated at specific altitudes that covered a .5 km by 1 km cross-shore area. The authors reflected the added high-capacity batteries and compact design were highly sought by casual past-timers (Brouwer et al., 2015). Capello, Guglieri, Quagliotti, and Scola (2012) raved on the four motors and capability of UAVs, deemed as quad-rotors that could hover in-flight with precision over urbanized locations. Whereas C. Cai, G. Cai, Xu, and

Zou (2016) described their interests in what they deemed as miniature aerial vehicles could withstand wind disturbances and obstacle avoidance during hovering maneuvers.

Along with the views of Brouwer et al. (2015), Capello et al. (2012), and Cai et al. (2016) on some of the UAV dynamics, Mack (2014) boasted on the thermal imaging characteristic of the MQ-9 Reaper. The MQ-9 could cause quite a stir if used in private entities because the surveillance vehicle was capable of detecting human body heat from approximately 37 miles (Mack, 2014). Kimantas (2014) noted image capture was successful using a gyro-stabilized aerial camera that was mounted on a drone; whereas Kim, Kwon, and Seo (2014) found the use of more than one UAV with a camera mounted on each provided somewhat of a stereo vision system aided in obstacle detection.

Pau, Tesoriere, and Tirrito (2015) observed performance factors in UAVs during operations, such as surveillance, and proposed the use of Fuzzy Logic Controllers (FLC) to regulate the UAV power. A reduction in battery power consumption prolonged a UAV’s battery life from 24-minutes to a 30% elongation of 30-minutes with FLCs (Pau, Tesoriere, & Territo, 2015). While Arquero, López-Granados, Peña, Serrano, and Torres-Sánchez (2015) review was an agricultural study, the high-throughput 3-D monitoring analysis netted in a time reduction when a taller altitude of 100-m was selected over a 50-m flight altitude during image collections and processing.

Drone Governance

Stahl (2013) noted camera functions of drones made a significant presence in military operations, entertainment, and domestic spaces through image captures and interactive gaming affected public rights, an ongoing revelation in drone laws constantly sought in international, national, federal, and local governance. Although Stahl’s article described drone challenges regarding rules of law in domesticated wars, no clear governance was discussed (Stahl, 2013). In Sterio’s (2012) drone analyses, the focus was more on Vogel’s view on the forceful use of drones during war under the auspices of the laws of war over constrained territorial locations.

Maryland law is not included due to the lack of applicable Maryland policies on drones and privacy, so situations involving Florida law were used. Miami-Dade Florida Police Department prescribed a handbook to its workforce that addressed a compilation of crime situations against state laws and statutes; in particular, drones used in surveillance, search, and seizure efforts (“Gray literature,” 2014). The handbook emphasized Florida’s Freedom From Unwarranted Surveillance Act with three notable exceptions for drone-use. In one exception, the Secretary of Homeland Security dictated drones could be used in high-risk acts, such as terrorist activities; a second exception was upon an approved search warrant by a law enforcement agency; and the third exception was for use of a drone without delay when a law enforcement agency acted immediately due to life endangerment or grave property damage (“Gray literature,” 2014).

Another perspective came from a Miami-Dade Florida County Attorney who issued a memorandum to the Board of County Commissioners which recommended the use of drones, specifically for convicted sexual predators who observe or record activities of minors, be met with criminal penalties (Price-Williams, 2015). The document relayed the need for additional convictions in light of state legislature that limited the use of drones by law enforcement organizations (Price-Williams, 2015). A month earlier, the same county attorney issued a memorandum aimed to protect Miami-Dade Florida airways from drone-use because of the imminent threats the devices caused in or near aircraft activities (Price-Williams, 2015). Price-Williams (2015) requested only a one-mile no-fly zone near Miami-Dade Florida runways, although Public Law 112-95 stipulated a 5-statute mile prohibition of drones away from locations with aviation activities (FAA Modernization and Reform Act of 2012).

According to FAA Modernization and Reform Act of 2012, Public Law 112-95, model planes, such as recreational drones, were to be flown under community-based safety rules under some form of nation-wide community-based auspice, restricted to 55 pounds, not to interfere with manned aircraft, and the operator must have received mutually-agreed upon and accepted operating instructions from the airport operator, as well as instructions from the control tower before the drone was operated within five miles of an airport. Whereas Marris (2013) noted FAA requires outdoor drone operators under research programs to apply for two certificates that assert drone flights are hazard-free to other aircraft, humans, or property. Although there were fewer restrictions on non-commercial drones, FAA stipulated the research drones could not be flown in flight paths around cities or populated locations (Marris, 2013).

Additionally, Neil and Neil II (2013) identified nearly “300 law enforcement agencies and research institutions which have temporary licenses from the FAA to use drones (including the Grand Forks SWAT team)” (p. 354). Stephens (2013) noted a group known as the Futures Working Group (FWG) possessed aspirations to tackle technological, legal, and societal issues that continue to rise in neighborhoods. Fourteen publications credited to FWG dealt with these issues; among them were augmented reality technology and neighborhood-driven policing (Stephens, 2013).

According to Creswell (2012), variables in quantitative studies can be derived from research titles; accordingly, variables could come to light in regards to the title of this research, “Drones: Discovering Perceptions of an Invasion of Privacy in Residential Areas”. Perception of a drone phenomenon; awareness of drone capabilities to violate privacy; or legal issues were used in the literature search. Some variables were considered for research, such as familiarity with applicable privacy rights, drone laws, knowledge of drones, and knowledge of common characteristics. Creswell (2012) also shared performing a qualitative study was quite fitting when variables were not known and required further exploration.

During their study, Calo et al. (2015) found contextual differences in one of their key variables, spatial data, which had connotations of spatial boundaries; yet, the same variable could have been used to classify owners and residents at home and in businesses. Vilalta (2012) found there were influences amongst variables, such as instances of the fear of crime in groups identified by age and gender. Once Caine, Fisk, and Rogers (2005) identified personal characteristics and image type as variables for privacy-related human factors, they monitored their research to capture emerging variables. Denscombe (2009) found certain variables, such as age, did not fare well when analyzing the data, although a respondent likely answered a question when it required little effort and the information was familiar. Erkip and Mugan (2010) noted people grouping, gender, income, and religion served to show how perceptions varied amongst variables of the same activities. Just as important, Armayor, McQueen, Vivar, and Whyte (2007) indicated certain variable terms should be contextually defined for explicit understanding and to avoid misconceptions.

Privacy Rights and Drone Laws

Applicable privacy rights and drones' laws could sometimes not be known or understood by different people. Crowsey et al. (2013) and Sanders (2015) shared similar views that drones could identify someone's location who was not a part of its surveillance or that a device could pick up the location of a resident through a window, which could be thought of as an invasion of privacy. Additionally, Crowsey et al. (2013) found differences in opinion amongst participants as to what constituted a violation of location privacy, when the authors voiced concern about the facial recognition program of a video company's surveillance and marketing scheme.

Knowledge of what laws apply in a given situation could influence one's behavior and the ability to avoid catastrophic ends. Takahashi (2012) questioned the handling and legality of a police-involved surveillance and arrest of a civilian on private property when a Predator drone was used to locate a suspect. Whether the suspect knew which rights applied in any instance is unknown, but for this study, finding out the participants' perception of applicable local, state, and federal laws aided in the overall research.

Chapter Conclusion

Higher educational portals, such as CTU library, provided a great number of entry points to electronic references, which included books and dissertations to support title searches, articles, research documents, and journals. However, Blalock and Gilchrest (2013) noted care and scrutiny must be exercised when using journals. UAS developments are on the rise with certain camera characteristics that make drones very appealing to consumers; additionally, they are considered to have a high return with educational investments (Brouwer et al., 2015; Terwilliger, 2013; Wolper, 2012). Reynolds (1978) and Sander's (2015) shared views of the Fourth Amendment, which asserted a person had the right to feel secure in their homes. Whereas acts of voyeurism remain illegal and there is the expectation of privacy that should be observed in personal places like bathrooms, as UAVs have shown up more rapidly over metropolitan areas for use in police activities, farming, and for recreational purposes (S. J-113-10: Futures of Drones, 2013).

Chapter Summary

The purpose of this qualitative phenomenological research was to understand how private citizens perceived privacy when drones flown over their residences could possibly access cyber devices operating within their homes. Chapter 2 presented different literary aspects on the perception of privacy experiences and identifiable details of drone characteristics as noted by Garton, Robertson, G. White, and S. White (2012). Challenges in the rule of law and drone analysis were presented, along with a review of what could constitute an invasion of privacy, and variations of literature reviews as hinted by Sterio (2012), Crowsey et al., (2013), and Sanders (2015) were made through different aspects into educational influences with drones.

Several research processes utilized led up to the literature review, which entailed compiling information gained from Chapter 1 and expanding on it in Chapter 2. The literature review provided an opportunity to present the problem and purpose statements that served as elementary contributions, while searches through titles, articles, and journals played major parts in queries and netted germinal information based on current and future technological developments. The compilation, selection, and analyses of selected documentation and findings, as appropriate, provided an avenue to grasp insight into existing literature. The intent of this qualitative phenomenological approach was to avoid falling into pitfalls of blurring collective details as Applebaum (2012) proposed happened previously with various qualitative researchers.

Chapter 3 outlines the methods used in the study to collect data to address the existing gaps in literature with respect to privacy in drone operations, cybersecurity, legalities, and education. The chapter continues by highlighting the research approach and design, geographic location, sample population, data collection techniques, selection method, and data analysis to explore the perceptions of privacy as they relate to drone activities. The chapter concludes with a summary of the research methods to support this study.

CHAPTER 3: RESEARCH METHODS

The purpose of this qualitative phenomenological research was to understand how private citizens perceive privacy when drones flown over their residences could possibly access cyber devices operating within their homes. Drone capabilities could be used to invade a person's privacy actions leading to unauthorized data sharing (Jacobstein, 2013). Numerous drones are now used to hover over areas of interests for recreational purposes where unlawful viewing and data collection of someone's private space could materialize, thereby jeopardizing privacy rights (Jacobstein, 2013; Choi-Fitzpatrick, 2014).

Overview

Chapter 3 discusses qualitative research methodology through descriptive characteristics of the research design, population, sampling, data collection, and data analysis used during this study. The research methodology and design allowed further elaboration on the research population, exemplified the form of sampling used, provided an understanding of the data collection procedures, and permitted the proliferation of data in a clear and organized manner as identified by Creswell (2012). Resource analyses identified in Chapter 2 were paramount and further allowed an understanding of the problem statement.

Applebaum (2012) suggested phenomenological researchers who critique pragmatic approaches distort partiality; however, in following Creswell's (2012) description of qualitative methodology, Chapters 1 and 2 demonstrated vital information that assisted in the continual quest of this research, created a solid foundation of the research methodology, and provided support to execute the research work. Cassell and Symon (2011) identified categorization of qualitative information be performed throughout an analysis and substantiation of discoveries to provide familiarization of the research approach. Revelation of literature gaps and insight into the research plan allowed outlining validation of internal and external processes led to a sound and successful study.

Research Method

As indicated in Chapter 1, a qualitative phenomenological research method allowed for the gathering of information on adult residential citizens regarding their perceived expectations of privacy through their cyber devices as related to drones operating nearby their homes. Quantitative and mixed methods showed some characteristics that could have been used in this study, however, qualitative proved most appropriate to perform this research. More so, Erkip and Mugan (2010) noted a qualitative research approach was most appropriate when gaps exist in the literature. Dilles et al. (2016) indicated qualitative researches served to draw out details of participant perceptions and experiences. Additionally, results from qualitative studies can be leveraged into quantitative studies, such as the authors’ table on population demographics (Dilles et al., 2016).

Qualitative methods tend to be structured in a fashion where the advantage is capitalized through interviews that net clarifications and permits documenting examinations attributed to the phenomenological insights gained from individual experiences (Akkoyunlu & Daghan, 2014). Dilles et al. (2016) used semi-structured interviews during their research to discover the significance behind their nursing empowerment phenomenon. For this research, 18 households were sought for interviews, 14 selected, keeping in-line with the small neighborhood grouping identified by Erkip and Mugan’s (2010) in their review of Haroldsen’s 1999 finding on qualitative research.

Applebaum (2012) implied qualitative research did not require participants be swayed by a phenomenon, but that participants be reflective of the actual phenomena without influence from their daily life activities. Melling and Slife (2012) noted three comparative, but limiting factors helped them realize limitations towards the phenomenon in their write-up: Variables may have existed that could not be translated into quantitative terms; participants may not have been able to relate their experiences against a number factor; and, while quantitative was advantageous for number comparisons, key details may have been omitted in order to fit experiences against the method, jeopardizing information that did not mold into the design.

Finfgeld-Connett and Johnson (2012) observed there seemed to be more quantitative researches completed than qualitative, so this completed study will be a valuable asset to qualitative research consortium. Further, mixed methods did not support the time allowance to perform this study and although no duration was mentioned, Shannon-Baker (2015) collected multiple sets of data simultaneously in a fashion that each data set maintained distinguishable traits, which were unaffected by the other sets during a concurrent parallel mixed methods study. Therefore, using data analysis through mixed methods did not support time-effectiveness for this study as Melling and Slife (2012) mentioned against time constraints.

Appropriateness of Design

The rationale for the proposed qualitative phenomenological research was to bring to the forefront the experiences and perceptions of participant experiences of privacy addressing private, individual drone operations initially observed around a South Florida residential area (Anonymous, personal communication, September 12, 2015). Addressing costs and time constraints, it was more advantageous to use a Maryland residential neighborhood instead of the Florida neighborhood. Creswell (2012) presented three research designs that could serve as primary purposes in the exploration of common experiences during a qualitative study; however, the phenomenological aspects of this research did not fall in line within any of the procedures for grounded theory, ethnographic research, or a narrative research. Instead, this study drew from a more psychological perspective that required greater detail about a phenomenon under observation based on data obtained directly from participants as Giorgi (2012) described through descriptive phenomenology.

Qualitative descriptive phenomenology was appropriate for this study because it supported the open-ended questions approach identified in qualitative research (Creswell, 2012); multiple open-ended questions were posed to participants of their perception of their own personal experiences. Shannon-Baker (2015) used journals based on open-ended questions in the qualitative portion of a mixed-study research. Creswell (2012) recommends interviews and questionnaires are reflective of qualitative narrative designs when there were unknown variables and limited information about a phenomenon in which opportunity is provided to gather participatory information through investigation.

The goal of using a phenomenological approach, specifically an interpretative phenomenological analysis (IPA), was to facilitate a comprehensive examination of experiences as demonstrated by Wagstaff and Williams (2014). Through an IPA, the intention was to recognize and discover participants' perception of drones flown in their reasonably expected private living areas without external influence. Open-ended questions were posed to participants in regards to their perception of their personal experiences through semi-structured interviews modeled after previous studies for small group participation as posed by Wagstaff and Williams (2014) and Anteunis, Joore, Linssen, Minten, and van Leeuwen (2013). The focus on discovering the meaning behind the phenomenon was the question, "what perceived privacy rights are associated with the private, individual use of drones operating in a Maryland residential area?" As demonstrated in Figure 1, Methodology Map, key input to answering this question was identification and selection of participants, determined sampling, data collection, and data analysis.

Population

The general population for this study involved a small diversified Linthicum Heights, Maryland neighborhood where only one adult was expected to participate from each of the selected 18 households. Creswell (2012) suggested information be collected on the study population to capture participant characteristics that could be used in surveys. Thus, narrative discussions were used to summarize findings of the analyses based on the phenomenon that addressed each resident's perception of their invasion of privacy experiences.

Englander (2012) rationalized identifying participants required a selection process to determine first, if candidate participants had the necessary experience to participate in the research, and to avoid any preconceived ideas behind the phenomenon. A small housing area was identified as the likely site because of the initial drone situation encountered by a South Florida resident; however, in the midst of this research, a Maryland neighborhood was identified to better query several candidates for participation. Englander (2012) implied once a site is selected and the general location narrowed down, sampling size would fall under scrutiny as participants were selected.

Sampling

The general population for this study involved an Anne Arundel County, Maryland neighborhood where the phenomenon occurred, using purposeful sampling as described by Creswell (2012). Barr, Bradman, Fenske, Whyatt, and Wolf (2005) assessed variability in four cases and demonstrated critical sampling as the most effective sampling method for their assessment. For this study, maximum variation permitted developing several perspectives based on the cultural diversity of the Maryland neighborhood; and as implied by Creswell (2012), this allowed information to be collected on the study population to capture participant characteristics for use in surveys and narrative discussions summarized findings of the analyses. Mort, Shelton, and Smith (2014) took advantage of another sampling method, purposive sampling, to narrow their research questions to a workable sample population.

Additionally, Creswell (2012) considered maximal variation sampling a form of purposeful sampling that could be used in data collection in qualitative studies. Maximal variation was a viable method for this study due to the small participant set. Size characteristic was a factor of sampling for this study based on the scope of the neighborhood, which caused the number of participants be targeted from 18 households with 14 selected.

Informed Consent

Protection of Human Subjects (2009) regulates informed consent where guidelines are set by the Code of Federal Regulations Title 45 (CFR); these guidelines were followed to protect participants’ confidentiality. Although no personally identifiable information was shared, a written statement preceded an electronic request via email to gain permissions required from each participant before questions were asked. Additionally, discussions included participants’ opinions, data collected from participants’ based on their personal observations and experiences, and researcher emails provided. Jones and Mealer (2014) included other information in their consent apparatus that covered details of their study, such as how long questioning was expected to last, a synopsis of the questions, possible pros and cons, as well as their contact information should the perspective participant were to inquire on the study.

An informed consent letter (Appendix B) was provided to and completed by each subject participant before the start of any interview; additionally, a copy of the signed consent letter was given to the participant for their records. The general requirements of CFR 45 for informed consent stipulated rules and instructions for a research, in particular, the following were abided: 1) a legal consent from the subject was attained; 2) the subject was made aware of his or her choice to voluntarily participate without coercion; 3) information was provided to each subject in understandable, plain English language; 4) there was no waiving of the subject's legal rights; 5) a description, purpose, and the expected timing of the subject's interview was provided; and 6) there were no monetary gain or incentives for participation. Lastly, permission from the CTU IRB was gained prior to making contact to prospective participants.

Confidentiality

Haahr, Hall, and Norlyk (2014) indicated it was most beneficial to the researcher to create trust relationships and ensure privacy when prepping to interview participants. Establishing trust and confidentiality were necessary in all interviews, but as explained by Goldman et al. (2013), preserving confidentiality and privacy were equally important. Creswell (2012) advised attention be made to details that may have presented ethical issues, such as obtaining consent and age requirements; therefore, care was given to prevent ethical issues, abstain from revealing personal data, and allowed protection of each participant's input against their identity.

All interviewees were requested to show they were at least 18 years of age prior to the start of an interview. No minors were included in this study. Personal contact during interviews provided protection of sensitive information and personal interviews conducted by telephone, email, and in-person permitted gathering the latest trends and information, as noted by Creswell (2012) and Jones and Mealer (2014).

Geographic Location

Goldman et al. (2013) noted comprehensive interviews resulted in detailed data with relative effect on the number of situations found at a study location. Metcalfe and Newington (2014) found researchers had to contend with potential problems in certain locations and speculated encountering additional problems in their selected study location; they also felt research staffing far outweighed importance over location. Even though the problem statement stemmed from a small South Florida residential neighborhood where a drone was found on a resident's private property, there was only one researcher for this study and the new geographic location of Maryland was still of equal importance due to the drone phenomena there. Regardless, this study targeted 18 households, 14 selected, with only one adult chosen as an interviewee from each residence.

Data Collection

Qualitative data collection required identification of participants and locations, appropriate access obtained, relevant data types determined, collection forms and tools developed, and the actual implementation and management of data processes, as described by Creswell (2012). Creswell (2012) noted qualitative data collection approaches consist of those under observation, interviews and questionnaires, documents, and audiovisual materials; however, observation was a challenge due to difficulty with site access, but still provided the opportunity to exercise open-ended questions and recording. There were other comparisons in data collection that contributed to the decision to use interviewing for this study, such as:

- difficulty establishing connections as a 1st-hand observer;

- although documents were good data sources of already transcribed information, efforts were quite exhausting when trying to locate and acquire documentation; and,
- despite participants’ immediate ability to relate to audiovisual materials of a phenomenon, the use of audiovisuals could have altered participants’ views and unadulterated input could have been jeopardized, as noted by Creswell (2012).

Creswell (2012) identified five process steps in qualitative data collection be performed in a sequential hierarchical manner. Therefore, data collection steps for this study consisted of the following:

- Purposeful sampling used to identify participants in a Linthicum Heights, Maryland neighborhood where a drone phenomenon occurred. Because of this phenomenon, a critical sampling strategy was posed; however, snowball sampling was considered in order to locate potential participants before the study was underway. Dilles et al. (2016) used snowball sampling when participating nurses identified others who shared similar experiences, which increased their study participants from three to 11.
- Permission gained from Capitol Technology University (CTU) Institutional Review Board (IRB).
- Protocols and instruments designed to collect and record data from participants.
- Data collection performed under the auspices of an approved proposal (predecessor to this document), while bearing in mind ethical considerations and emerging questions formed from the protocols.

Cleary, Horsfall, and Hayter (2014) considered interviews as the most common qualitative data collection, whether performed in a group environment or one-on-one. Cleary et al. (2014) noted of the seven challenges inexperienced interviewers tend to face, use of surveys and interviews were still the two most advantageous approaches to take for this study. Anteunis, Joore, Linssen, Minten, and van Leeuwen (2013) indicated interview techniques were used in their data collection through open-ended questions in sessions of less than one hour per participant allowed them to have normal conversations and promoted increased dialogue.

Aside from consent forms, interviews and questioning were the prime focus as participants were approached with electronic copies of the online questionnaires (Appendix C). Denscombe (2009) used a combination of online questionnaires and paper-based questionnaires to survey participants. Sound ethical safeguards provided confidentiality and privacy was maintained throughout the research began with each transcribed interview, which was accounted for and stored on a microSD chip, placed in a sealed envelope, and maintained in a locked filing cabinet until disposition. After the 3-year filing period, the material will be properly disposed of and destroyed by pulverizing or burning (as appropriate for the type of material).

The interview protocol designed to help the administration of interviews kept the interview focused and aligned with instructions during the research as suggested by Creswell (2012). Questions posed to participants consisted of open-ended queries where participants provided responses of their own interest in drones. Semi-structured interviews were employed to capitalize on techniques used in previous studies for small groups of participants in qualitative research as suggested by Wagstaff and Williams (2014); and Anteunis et al. (2013). Certain information had to be established at the beginning of the interview, such as demographics which Chur-Hansen, Crawford, and Ng (2014) obtained for their semi-structured interview and data collection. Sessions were recorded using audiotape for a detailed recount of each interview; however, there were no emerging questions. Collection in this qualitative research was query-focused on objective data retrieval, data where there were no right or wrong answers.

Use of protocols, as suggested by Creswell (2012), helped in the data collection and recording of all of the participant interviews through an acceptable saturation. According to Finfgeld-Connett and Johnson (2012), saturation of data collection occurred when complete explanations between conceptual views were attained from perceptive and arduous combing of research information. The authors noted not having enough studies available had an effect on saturated findings (Finfgeld-Connett & Johnson, 2012); however, Knapik (2006) completed a qualitative research using 90-minutes of recorded interviews collectively from only four participants.

Saturation occurred in this study when no new information was identified from the 14 completed surveys collected from the 18 households sought. Mort et al. (2014) exercised thematic saturation of data collection until no new data was being produced. The findings of this phenomenological study helped identify residents' perceptions of privacy with their cyber devices if drones were flown in their reasonably expected private living areas. Jones and Mealer (2014) identified demographics and employment-related questions to their survey before beginning interviews, which allowed them to get the appropriate data from qualified participants. The kind of data collected avoided participants from being led to provide canned answers, so the following questions were generated from the three research questions; first, to screen and identify the appropriate participants with apt subject knowledge, and secondly, to draw out in-depth details about the phenomenon:

- Are you 18 years old or older? A United States government identification card (I.D.), e.g. military I.D. or state driver’s license, was acceptable forms for proof of age. As previously indicated in this writing, anyone under 18 would be excluded and the interview would cease as soon as this was acknowledged.
- Do you know what a drone is?
- What do you know about drones?
- Have you experienced or seen drones flown in any residential area?

Subsequent questions included:

- How do you feel about new capabilities for special deliveries of packages to your residence using drones?
- How would you feel about quick deliveries by drones to your residence and giving up on your privacy to have such a delivery made?
- What notification methods would allow you to feel deliveries by drones is acceptable (e.g. phone calls or text messages made with at least a day’s notice)?
- What are some of the cyber devices that you use?
- What do you know about drones or UAS’ being flown in residential areas?
- How do you feel about a drone flying within your residential private spaces that could access any one of your cyber devices?
- What are some of your concerns of drones being flown within the confines of your reasonably expected private areas?
- How do you feel about local law enforcement on drones flown in residential areas? State? Federal?

- How can policy be implemented to ensure your privacy is not intruded upon during drone operations?
- Using a scale of 1-5, 5 being the most invasive, how would you rate drone operations in residential areas?
- What is your knowledge of zoning restrictions by areas, e.g. county, city, or state?
- How would you describe the no-fly zone policy?
- What fines do think would be reasonable when a drone operator invades your reasonably expected private space?
- What legal measures do you envision can be implemented to block or jam unwanted drones from intruding your reasonably expected private spaces and accessing your cyber devices?

Instrumentation

Fawcett (2011) voiced instrument selection was commonly considered a formidable and time-consuming task and other things, e.g. linguistic translation, might need to be considered in order to attain cultural relevancy. Knapik (2006) discussed the importance of researcher reactions and how interviews continue following participant responses while trying to keep interviewer reaction from affecting those responses. Comparably, Englander (2012) observed subject-to-subject relations, surveys, and psychological tests are a part of natural sciences for use in interviews relative to instrumentation.

Wagstaff and Williams (2014) and Anteunis et al. (2013) identified semi-structured interviews as instrumentation used in small group studies during qualitative research. Harrington, King, and McCloud (2013) completed an unstructured interview that lasted up to two hours and that time was driven by the participant’s desire to share inclusive information about their experience. Erkip and Mugan (2010) indicated the value of their interviews provided a more in-depth understanding following the completion of time-use surveys.

According to Creswell (2012), quantitative research is used to examine validity and reliability of data, whereas rigor is used to ascertain assurance in qualitative research. Considering cultural interests and an increase in technological development, researchers commonly seek instrument reliability and validity during planning efforts (Fawcett, 2011). According to Englander (2012) tradeoffs of non-measureable psychological qualities are expected in assured autonomous observer instrumentation.

Englander (2012) noted researchers should probe for the prospective subject knowledge level of the phenomenological topic to help with selection of participants. Erkip and Mugan (2010) indicated rework could extend research times and require follow-up interviews as demonstrated when the researchers noted recording errors during data collection. Mort et al. (2014) indicated rigor and reproducibility should be realized during data analysis, with which use of checklists helped keep the research information aligned with the methodology and repeatability.

Reliability and Validity

Applebaum (2012) wrote, “regarding validity in qualitative research, it ought to be noted that generalizability of research findings is not argued by means of statistics, but in terms of meaning” (p. 48). Since this was a qualitative research, understanding rigor versus internal and external validity, and such terms of meaning was noted from participants’ recount of their own life experiences (Magilvy & Thomas, 2011; Applebaum, 2012). According to Creswell (2012), internal and external validity are primarily used in quantitative studies to support experimentation and generally controlled to establish cause and effects in quantitative designs.

Clark and Creswell (2011) also discussed relational qualities between cause and effect in experimental studies, which are primarily applicable when a study is against a greater populace involving survey designs. Creswell (2012) identified internal, external, statistical conclusion, and construct as types of validity in quantitative studies. However, the intent of this writing was to provide details that permitted qualitative rigor, such that the research was seamless and methodologically unified between data collection and data analysis as described by Englander (2012).

Internal Validity

Creswell (2012) stated internal and external validity were two primary threat areas where inferences drawn must be based on factual or accurate data. Quantitative research allows the examination of internal validity for reliability of information collected, as well as source reliability (Creswell, 2012). In retrospect, a list of inferred threats related to the research problem would have been included if the research proposal was diverted to experimentation.

For this qualitative study, however, information was sought based on rigor discovered regarding the phenomenon under study promoted advancement of knowledge and development of practices of concern to participants, as noted through interviews (Magilvy & Thomas, 2011). A Lincoln and Guba model shared by Magilvy and Thomas (2011) was used to show the research reliability of the qualitative rigor through credible, dependable, transferable, and confirmable means. While credibility can be recognized through a single accurate interpretation of participants' experiences (Magilvy & Thomas, 2011), Dilles et al. (2016) noted credibility could also be demonstrated through two researchers, each analyzing a separate discipline of the data.

Tape recordings were made of each interview in their entirety once the prospective interviewee signed the consent form. There were no handwritten notes taken that provided clarification or additional details a participant did not want recorded electronically, although tape recordings and notes would have been transcribed into one interview transcription. Using the SurveyMonkey survey and analysis tool, as well as, extreme care in transcriptions permitted external validity of the study. The analysis was dependent on the singular, but accurate, dependable, transferable, and confirmable analysis of participant interviews included transcription of audio recordings and notes.

External Validity

Just as threat factors exist in internal validity, there were threats for external validity where certain information could have been considered degraders or discriminating factors to research outcome; such factors were disregarded since they could ultimately alter the results of the study as implied by Creswell (2012). Further, it is problematic when researchers displace or improperly infer external validity threats, such as sample data against individuals or situations (Creswell, 2012). Researchers should factor in deciphering and deliberating internal and external threats to control and eliminate such threats at the beginning of validation (Harris, 2013; Creswell, 2012). Several actions were taken to provide accurate inferences from generalized survey results: 1) surveys were delivered in a convenient, electronic online fashion; 2) generalizations included different settings, such as experiences from different areas inside of and around the home; and, 3) results were generalized based on two different events, Father's Day and the 4th of July.

Data Analysis

Numerous data analysis tools were considered to analyze data collected from participating interviewees. Eckartsberg (2010) noted personal experiences can be used in data analysis through some form of representation based on a person's perception of their experience while noting if there were any personal senses applied, e.g. hearing, touching, etc. Snelgrove (2014) indicated the objective of an interpretative phenomenological analysis (IPA) study was to illustrate the comprehensive evaluation of participants' experiences in certain situations. The decision to use IPA helped answer the three main research questions:

- How do residents feel if faced with a drone flying within their residential private spaces and accessing their cyber devices?
- How do residents feel about drones entering their private spaces, collecting data about them, and placing that data in the cloud?
- How do residents feel regarding law enforcement's handling of drones flown in residential areas?

Data analysis steps identified in Figure 1 included transcribing interviewee recordings, questionnaires, and researcher notes; completing data entries into SurveyMonkey data analysis tool; setting up the coding and categorization on the data collected; and, data organization into themes for further interpretation. IPA was considered because it allowed detailed reflections of each participant's recount of their experiences as advocated by Wagstaff and Williams (2014). Cassell and Symon (2011) and Creswell (2012) suggested performing personal interviews to draw together original, chronological, and quality recollection of participants' experiences could be transcribed with confidentiality into themes for data analysis. Wagstaff and Williams (2014) summarized themes from participants' input and demonstrated a triangular layer of progression through research interviews, clarification interviews, and post meetings further led to a set of emergent themes.

Existing literature lacked specific and in-depth data on individual perceptions of experiences gained in drone usage within residential areas, so data analysis modeled several interpretative phenomenological steps exercised by Wagstaff and Williams (2014). Progression and analysis tracking was used to comb through and listen to each participant's interview of recorded audio. Code verification was exercised as each transcript was saved into Microsoft Word documents and then the recorded data securely and physically protected. Digital formats supported establishing emergent themes using the SurveyMonkey apparatus and the same tool used for data review and clarification. This iterative process permitted identifying material for comment, further massaging of themes, as well as, arranging clarifying post-interview meetings to discuss and reach a finalized thematic research set, which ultimately led to a summary of lessons-learned about the phenomenon as speculated by Wagstaff and Williams (2014).

Chapter Summary

Chapter 3 provided details of the planned research method, explained the research design, identified the population, sampling, informed consent, geographic location, data collection, instrumentation, reliability and validity, and data analysis. Themes, as demonstrated by Mort et al. (2014), were created from data transcriptions derived from journals, recordings, and questionnaires, which avoided preconception of thematic ideas prior to the study that could have swayed the study's outcome. Erkip and Mugan (2010) noted a qualitative research approach was most appropriate when gaps existed in the literature.

This qualitative phenomenological study supported an open-ended questions approach as Creswell (2012) identified in qualitative research. The general population involved a small

Linthicum Heights, Maryland residential neighborhood where one adult was sought from 18 households, 14 selected. Sampling was based on size characteristic, the scope of the neighborhood, and receipt of informed consent in accordance with CFR 45, 690.116. This study was expected to reach saturation when enough information was gained from 14 adult participants using data collection techniques through open-ended questions, as noted by Anteunis et al. (2013). Furthermore, it was intended this qualitative research be seamless and methodologically unified between data collection and data analysis as advised by Englander (2012), and of rigor through participants' own recount of their life experiences, as proposed by Magilvy and Thomas (2011).

Chapter 4 discusses the specific details of the procedures used in this phenomenological study. The chapter presents data collected through the surveys and interviews. The chapter concludes with research findings.

CHAPTER 4: RESULTS

The purpose of this qualitative phenomenological research is to understand how private citizens perceives privacy when drones flown over their residences could possibly access cyber devices operating within their homes. Gaps were found to exist in current information following the literature review of drone capabilities that could allow an invasion of a person's privacy through authorized or unauthorized cyber devices. Chapter 4 contains a discussion of how study results materialized, details the SurveyMonkey tool through instrument validation, discusses the findings based on the outcome of electronic questionnaires and interviews, categories, and themes.

Participants were selected from a Linthicum Heights, Maryland neighborhood where 18 residential homes were targeted for participation in the study, 14 selected. Data collection included an online survey of specific questions as shown in APPENDIX C, which was created using SurveyMonkey, distributed to participants, and followed by three to 15-minute semi-structured interviews. Interviews allowed amplification of participants' responses based on their perceptions of drones and how they perceived acts against their privacy. Over 35 tables illustrate the content analyses of survey responses to address the study's three main research questions. To demonstrate the phenomenological viewpoints of participants, responses were captured and organized categorically.

APPENDIX D demonstrates relational concerns categorically and thematically of how participants described feelings of a phenomenon based on their perceived drone experiences. There is a breakdown of each theme containing several of the 17 categories of information: (a) (C01), Cybersecurity; (b) (C02), Cybersecurity Policies; (c) (C03), Cybersecurity Practices; (d) (C04), Cybersecurity Training; (e) (C05), Delivery Notifications; (f) (C06), Drone Package

Deliveries; (g) (C07), Education; (h) (C08), Fines; (i) (C09), Law; (j) (C10), Law Enforcement; (k) (C11), Notifications; (l) (C12), Permission; (m) (C13), Policies; (n) (C14), Privacy; (o) (C15), Remote Access; (p) (C16), Reporting; and, (q) (C17), Technological Implementations.

Analysis and grouping of related participant responses showed the 17 categories further resulted in four major themes. Theme 1 (T1), made up of cybersecurity practices relayed how participants felt of their residential domains. Theme 2 (T2), made up of laws, policies, law enforcement, fines, notifications, and reporting revealed what participants perceived against their private residences. Theme 3 (T3), made up of how residents perceived they felt in order to be better informed, educated, and trained on cybersecurity. Theme 4 (T4), made up of how participants perceived they felt about possibilities of drone capabilities to deliver packages to their residential areas.

Instrument Validation

Instrumental advice provided by several peers ensured survey questions and interview sessions appropriately addressed qualitative phenomenological aspects of this study in a clear and concise manner. Order of survey questions was modified based on recommendations permitted an easier flow for survey understandability. Demographically, 33 adults from 18 households were asked if they would like to participate in the study; 14 respondents completed the online surveys, 12 submitted to personal interviews; thus, two of the 14 respondents were unable to meet for interviews and offered electronic interview responses.

Demographics

Makeup of participants ranged in age, ethnicity, sex, and profession as illustrated in Table 1, Demographics, which were drawn from survey questions 1-12, Tables 2-13.

Table 1: Demographics

Participant	Age	Ethnicity	Sex	Years of College	Profession
1	55-64	Other	M	2	Local Government
2	35-44	White	M	4	Law Enforcement
3	25-34	White	M	Some Graduate	Computer & Mathematical
4	35-44	White	M	Graduate School	Architecture & Engineering
5	25-34	White	M	Graduate School	Computer & Mathematical
6	45-54	White	M	1	Management
7	35-44	White	M	4	Business & Financial Operations
8	35-44	White	M	3	Sales
9	35-44	White	F	Graduate School	Education, Training, & Library
10	18-24	Asian	F	1	Student
11	35-44	White	F	Graduate School	Government Policy
12	35-44	White	F	Graduate School	Education, Training, & Library
13	35-44	White	F	2	Business and Financial Operations
14	25-34	White	F	2	Stay at Home Mom

Note. M = Male; F = Female.

Questions 1-12 were demographically based and prompted background information about participants. One hundred percent of the 14 responding participants agreed to participate in the study and actually completed the 39-question online survey identified in Table 2, Question 1. Two committing residents later requested their spouses receive the survey instead; so subsequently, the survey was distributed to a total of 16 residents. Although four adults from two different households received the surveys, only one adult participated per household.

Table 2: Question #1 – Survey Participation

Would you like to participate in this survey?

Content Analysis: This first online question provided the participant an opportunity to opt out of the survey by selecting *no*, which caused the online application to quit; all participants selected *yes* and were able to complete the survey.

Answer Options	Response Percent	Response Count
Yes	100.0%	14

The majority of participant's (57%) were ages 35-44, 7.14% were 18-24, 21.43% were 25-34, 7.14% were 45-54, 7.14% were 55-64, and there were no participants 65 and older as identified in Table 3 for Question 2. All 14 participants gave permission for taped interviews (Table 4, Question 3) and although two were unable to meet in-person, they both provided paper responses to interview questions; the remaining 12 met in-person for interviews. Tables 5 and 6 contained respondents first and last names (Questions 4 & 5, respectively), which were not identified in this document for confidentiality purposes. All participants lived in Linthicum Heights (Table 7, Question 6), Maryland (Table 8, Question 7); however, for privacy purposes, participant names were excluded from this report and were only gathered for future contact and follow-up.

Table 3: Question #2 – Age Range

What is your age?

Answer Options	Response Percent	Response Count
18 to 24	7.1%	1
25 to 34	21.4%	3
35 to 44	57.1%	8
45 to 54	7.1%	1
55 to 64	7.1%	1

Table 4: Question #3 - Permission to Record

Do you give your permission to have a tape-recorded interview of this survey? An interview will allow the interviewer to go through the survey with you and provide clarification on any unanswered questions in the survey.

Content Analysis: A *no* response would have directed the researcher *not* to attempt to record the interview session that would follow; however, all respondents answered *yes*.

Answer Options	Response Percent	Response Count
Yes	100.0%	14

Table 5: Question #4 - First Name

What is your first name?	Response
All Respondents answered	Names masked for confidentiality.

Table 6: Question #5 - Last Name

What is your last name?	Response
All Respondents answered	Names masked for confidentiality.

Table 7: Question #6 - City

In what city do you live?	Response Percent
Linthicum Heights	100.0%

Table 8: Question #7 - State

What state do you reside in?	Response Percent
Maryland	100.0%

Over 85% of participants were White, 7.14% of Asian decent, and 7.14% noted multiple ethnicity identified in Table 9, Question 8. There was a close showing between male and female participants with 57.14% male and 42.86% female shown in Table 10, Question 9. All participants garnered high school education and at least one year of college. Graduate school participants topped at 35.71%; a tie for one year of college and 4-year college degrees at 14.29% each; as well as a tie for 3-years of college and participants with some graduate school at 14.29% each shown in Table 11, Question 10.

Table 9: Question #8 - Ethnicity

Which race/ethnicity best describes you? (Please choose only one.)

Answer Options	Response Percent	Response Count
Asian / Pacific Islander	7.1%	1
White / Caucasian	85.7%	12
Multiple ethnicity / Other (please specify)	7.1%	1

Table 10: Question #9 - Gender

What is your gender?	Response Percent	Response Count
Female	42.9%	6
Male	57.1%	8

Table 11: Question #10 - Education

What is the highest level of education you have completed?

Answer Options	Response Percent	Response Count
1 year of college	14.3%	2
2 years of college	21.4%	3
3 years of college	7.1%	1
Graduated from college	14.3%	2
Some graduate school	7.1%	1
Completed graduate school	35.7%	5

Current occupation of respondents ranged from management, business and financial, computer and mathematical, education, training and library, and sales, to other occupations, such as stay-at-home mom, government, student, and law enforcement as shown in Table 12, Question 11. Respondents shared combined household salary ranged from $100k to over $200k, excluding 42.86% of respondents who chose not to answer as shown in Table 13, Question 12.

Table 12: Question #11 - Occupation

Which of the following best describes your current occupation?

Answer Options	Response Percent	Response Count
Management Occupations	7.1%	1
Business and Financial Operations Occupations	14.3%	2
Computer and Mathematical Occupations	14.3%	2
Architecture and Engineering Occupations	7.1%	1
Education, Training, and Library Occupations	14.3%	2
Sales and Related Occupations	7.1%	1
Other: Stay at home mom, local government, government policy analyst, student, and law enforcement	35.7%	5

Table 13: Question #12 - Income

How much total combined money did all members of your HOUSEHOLD earn last year?

Answer Options	Response Percent	Response Count
$100,000 to $124,999	14.3%	2
$125,000 to $149,999	7.1%	1
$150,000 to $174,999	14.3%	2
$175,000 to $199,999	14.3%	2
$200,000 and up	7.1%	1
Prefer not to answer	42.9%	6

Findings

Three research questions guided the execution of this study and provided an understanding of how private citizens perceived privacy when drones flown over their residences could access cyber devices operating within their homes:

- How do residents feel if faced with a drone flying within their residential private spaces and accessing their cyber devices?
- How do residents feel about drones entering their private spaces, collecting data about them, and placing that data in the cloud?
- How do residents feel regarding law enforcement's handling of drones flown in residential areas?

As shown in Table 14, research question #1, "How do residents feel if faced with a drone flying within their residential private spaces and accessing their cyber devices?" allowed respondents to think about their perceptions if a drone accessed their information through their cyber devices. Survey question #32 revealed 35.7% of respondents felt highly threatened by drones flying over or near their homes with the possibility of receiving wireless signals from cyber devices within their homes. All 14 participants responded; two felt little to no threat from drone activities.

Table 14: Research Question #1

How do residents feel if faced with a drone flying within their residential private spaces and accessing their cyber devices?

Below are respondents' comments to survey question #32:

- Dishonest people can purchase drones for neighborhood surveillance, i.e., monitor times of least inactivity of residents;
- I don't like my privacy being affected;
- Because it is not a problem in my neighborhood;
- Depends on the operation really;
- I feel it is an invasion of privacy;
- I don't feel its much more invasive than a vehicle driving by. I expect that I am responsible for securing wireless networks adequately.

As shown in Table 15, research question #2, revealed respondents felt they had a deeper concern when they thought about the advanced advent of technological capabilities of data discovery and collection. Survey question #17 revealed respondents' perception to how data could be gathered from many wireless devices within their private spaces and respondents were further alarmed at the mere thought that signals could carry a myriad of their information to unknown places.

Table 15: Research Question #2

How do residents feel about drones entering their private spaces, creating data about them, and placing that data in the cloud?

Respondents felt concerned with lack of awareness, invasion of privacy, and legalities as identified in survey question #17. Participants were even more alarmed when they thought about the possibilities of access and information gathering from their cyber devices and shared the following comments:

- I feel those actions are a violation of my privacy, not in agreement of that.
- Unless governed by a search and seizure warrant for a criminal investigation illegal.
- Collecting data about my internet-connected devices is nothing new, wardriving has been and still is a very good way to collect intelligence on devices with radios built in. So, in all honesty...so long as the aerial vehicle is being flown carefully and doesn’t endanger my family or property and it is not being done excessively I don't mind at all. I believe it is up to the owner of any devices with radios to understand how they work and properly protect them. I also do not really believe that any space outside the walls of my house can be considered private, so pictures and other data that can be collected is really my own responsibility.
- As long as all of the activities are legal, I am ok with it. I don't think it should be legal for a drone to fly within view of your windows while over your property boundaries.
- I'm incredibly nervous about this. Need to rethink how to ensure my network is setup to prevent these types of attacks.
- I do not think it should be legal.
- This practice makes me a little uneasy. However if it's for the purpose of public safety I am less bothered.
- I was not aware of that, but I don't agree with them doing that.
- It is always concerning because you are not aware of who will be able to access that information.
- I would be very concerned if this was done without my consent.
- Not good - invasion of privacy.
- It's unsettling.
- Against it.
- It makes me uncomfortable.

As shown in Table 16, research question #3 discussed respondents’ perception and comments to survey question #31 where the majority of participants felt they knew of no legal vehicle that allowed law enforcement to impose any law in situations where drones were flown in residential areas. Respondents also indicated perceived concern in survey questions #27-29 for local, state, and federal cybersecurity/wireless policies that could regulate the flying of drones in private areas, but respondents further indicated there would be challenges to manage and enforce such policies.

Table 16: Research Question #3

How do residents feel regarding law enforcement's handling of drones flown in residential areas?

There was mutual agreement among respondents to a lack of knowledge on legal handling of drones or even if there were laws governing law enforcement's handling, as demonstrated in the below comments to survey question #31:

- Nothing, not sure if the local law enforcement have much concern over drones.
- None.
- Nothing.
- Nothing.
- I know that in certain areas law enforcement has shot down drones. As for residential areas, I have not heard anything. But I'm sure they would be able to stop any drones if need be.
- I do not know how this is handled.
- I am not aware of any of these situations and how they should be handled
- I am not aware of law enforcements policies
- I do not think that they can do anything.
- From my understanding, law enforcement is very restricted in how it can handle drones. There is not a lot being done to stop them.
- Nothing.
- Nothing, I am not aware of our local police using devices like that for aerial reconnaissance.
- None.
  However, it would be a useful tool to use for surveillance in difficult to reach locations that would otherwise compromise an investigation. However, I'm sure laws or procedural ordinances would govern its use.

Analyses of participant responses were grouped into four major themes based on participant perceived experiences: (a) T1, cybersecurity practices; (b) T2, laws, policies, law enforcement, fines, notifications, and reporting; (c) T3, residential education in cybersecurity; and (d) T4, package deliveries by drones. The 17 categories of information were further matched to one of the four themes and described in each thematic section. APPENDIX D captures these details identified by theme numbers T1-T4 and categories C01-C17.

Theme 1 (T1): Cybersecurity practices

Based on the thematic class, theme 1 cybersecurity practices, responses regarding participants' perceived practices in residential cybersecurity were obtained from all 14 participants against survey questions 18, 19, 23, 33, 37, and 38. Respondents described their cybersecurity practices for new Internet or web-enabled cyber/wireless devices that entered their residential spaces. They noted precautions they felt would be needed to securely perform sensitive activities (e.g. banking) when using cyber/wireless devices. Participants described how they felt a no-drone-zone policy for drones could be applied to residential areas and identified what kind of cybersecurity training they felt was needed for residences to become more knowledgeable of wireless connectivity capabilities with drones flying in residential neighborhoods. Responses were classified into three categories: (a) cybersecurity, (b) cybersecurity practices, and (c) technological implementations.

a. Cybersecurity. Several participants perceived they had a good understanding of cybersecurity and mitigating strategies minimized risks to their wireless signals through blocking, jamming, or encryption. One participant felt a system shutdown would suffice, another participant felt collection of wireless signals could not be stopped; yet, another felt cybersecurity could be handled through service providers. DHS (n. d., Cybersecurity 101) noted users should exercise an understanding of risks and threats to their cybersecurity environment since the Internet is available through boundless means.

b. Cybersecurity practices. The majority of participants perceived they had a good sense in exercising some form of cybersecurity practices through segmented and controlled domains, guest connections, pre-shared keys and passwords, and took precautionary measures during online activities. Four respondents perceived there was very limited amount of available literature and announcements for home users and training was needed for residences to become more knowledgeable of wireless connectivity capabilities with drones flying in residential neighborhoods. DHS (n.d., Cybersecurity 101) issued five cyber tips to users: practice password discipline, keep systems updated, promote open user communications on safe Internet use, restrict personal information sharing, and use selective judgment on Internet or online offers.

c. Technological implementations. Seven participants felt technological implementations and controls could secure their web-enabled cyber devices from drones flying around their homes, such as altitude restrictions, time of flight restrictions, distance from home restrictions, laws and policies to protect privacy from drones, to some form of jamming device or encryption of personal traffic. One participant felt a technological solution integrated location of residential homes into the drone applications could be used to distinguish homes in a no-drone-zone implementation. Although the FBI (2016) actively targets malicious cyber activities, the bureau encouraged personal ownership of cyber security.

Theme 2 (T2): Laws, policies, law enforcement, fines, notifications, and reporting

Based on the thematic class, theme 2 laws, policies, law enforcement, fines, notifications, and reporting, responses regarding participants’ perception of legalities on cybersecurity in residential areas were obtained from all 14 participants. Classifications were made against participants’ input through survey questions 17, 20, 21, 23, 27, 28, 29, 30, 31, 32, 33, 34, 36, and 38. Responses were classified into 10 categories: (a) cybersecurity policies, (b) fines, (c) law, (d) law enforcement, (e) notifications, (f) permissions, (g) policies, (h) privacy, (i) remote access, and (j) reporting:

a. Cybersecurity policies. Respondents shared legal measures they felt could be implemented to block or jam unwanted drones from capturing wireless signals from their residences. They noted local, state, and federal cybersecurity/wireless policies they were aware of that regulated the flying of drones in residential areas. Participants also noted what kind of wireless policy they felt could be implemented to ensure web-enabled cyber devices were not intruded on when there was a drone flying around their home.

b. Fines. Respondents identified what they considered to be reasonable fines to impose on operators when a drone attempted to connect to residential cyber/wireless devices. Two participants felt no fines should be imposed on operators when their drone attempted to connect to residential cyber/wireless devices. Twelve respondents felt fines ranging from $300-$25,000 should be imposed on operators when their drone attempted to connect to residential cyber/wireless devices.

c. Law. With the exception of one participant, all respondents felt it illegal or a violation of their privacy when drones entered their private spaces, accessed their cyber/wireless devices, created data about them, and placed that data in a cloud. Respondents also cringed at the thought of their information collected without their knowledge and placed in some unknown location. Four participants indicated they wanted changes in law, anonymous reporting, and penalties as a result of this study when asked what they you expected from the results of this study.

d. Law enforcement. One respondent indicated fines and jail time could be a deterrent to unwanted capture of wireless signals when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence. Three felt law enforcement or another local authority, but not a homeowner's association, should address the flying of drones and any attempt to connect to residential cyber devices within residential neighborhoods. Although one respondent felt little could be done to address law enforcement's handling of drones flown in residential areas.

e. Notifications. Four participants had no idea of whom they would call if they suspected unauthorized activity on their cyber/wireless devices. Six indicated they would contact a law agency, such as the police or FBI, or their Internet Service Provider for suspected unauthorized cyber/wireless activities. Only one indicated such activity would warrant contacting Federal Communications Commission (FCC) or FAA.

f. Permissions. Several participants noted which cyber/wireless device and the actions they felt their service provider could remotely perform to control devices without the resident's permission or knowledge. Eight participants indicated their service providers could remotely perform updates or some action to their cyber devices without their knowledge. Five were unsure what cyber/wireless device or actions their provider could take to remotely control their device without their permission or knowledge.

g. Policies. Participants noted local, state, and federal cybersecurity/wireless policies they felt they were aware of that regulated the flying of drones around their homes.

One participant indicated handling of unwanted capture of wireless signals could be handled through policy that could allow blocking or jamming of unwanted drones from capturing residential device wireless signals. A couple of respondents felt a no-drone-zone policy could be applied to residential areas; although two felt even if there was a no-drone-zone policy for drones in residential areas, it would be difficult to enforce.

h. Privacy. With the exception of one, respondents felt it illegal or a violation of their privacy when drones entered their private spaces, accessed their cyber/wireless devices, created data about them, and placed that data in a cloud. They also cringed at the thought of their information collected without their knowledge and placed in some unknown location. Only 35.7% of respondents felt drone operations in residential neighborhoods were highly invasive. Yet, one respondent (highly educated in cybersecurity and drones) felt protection of cyber devices and privacy was homeowner responsibilities.

i. Remote access. Five respondents were unsure of any action their service providers could take remotely to control their cyber/wireless devices within their residential domain. Eight indicated their service providers could remotely perform updates or some action to their cyber devices without their knowledge or intervention. FBI (2015) issued a Public Service Announcement on dangers of IoT in cybercrimes, which contained information on IoT devices that could be used remotely to jeopardize security, such as smart appliances, security alarm systems, and wearable fitness devices.

j. Reporting. There were varying perceptions when asked who participants would call or notify if there were suspected unauthorized activities within their residential domain, such as unauthorized surveillance or possible electronic ransom. Four participants indicated wanting some type of vehicle that could allow anonymous reporting of activities when participants felt were a violation to their privacy, whether by drones or other wireless technology. Aside from FCC or FAA, one respondent noted an alert could be made to whoever was affected during the breach, as well as notification to the service provider.

Theme 3 (T3): Residential education in cybersecurity

Based on the thematic class, theme 3 residential education in cybersecurity was derived from responses from 14 respondents regarding participant's perception of their residential training, education, and awareness. Classifications were made against participants' input through survey questions 13, 14, 30, 37, and 38. Analysis of each response is demonstrated in Tables 17, 18, 34, 41, and 42. Responses were classified into two categories: (a) cybersecurity training, and (b) education.

a. Cybersecurity training. Three respondents were unsure of training deficiencies in cybersecurity in their neighborhood when asked what kind of cybersecurity training, they felt was needed for residences to become more knowledgeable of wireless connectivity capabilities with drones flying in residential neighborhoods. Nine respondents felt some form of announcements, notices, education and awareness, informative meetings, and training were needed. As of this writing, DHS (n. d., Cybersecurity 101) recently implemented a national awareness campaign to address people in their home, work, and school environments on cybersecurity.

b. Education. When asked what they felt they knew or understood of cybersecurity, eight respondents felt they were quite knowledgeable and understood uses and capabilities of drones and UAS’. Three felt they knew very little about drones and cybersecurity, but three felt they had no experience at all. DHS (n.d., Cybersecurity 101) noted its effort underway to educate families, employees, and those in educational environments on risks in public or personal cyber environments, tips that could be taken, and actions victims could take in any of the aforementioned situations.

Theme 4 (T4): Package deliveries by drones

Based on the thematic class, theme 4 package deliveries by drones, responses regarding how participants perceived drone capabilities to deliver packages to residential areas were obtained from all 14 participants. Classifications were made using participants’ input through survey questions 24, 25, and 26 and responses were classified into two categories: (a) delivery notifications, and (b) drone package deliveries.

a. Delivery notifications. Varying responses were received when asked what notification methods participants felt could be used to make wireless deliveries by drones to their homes acceptable. Some respondents were totally opposed to such deliveries and felt no notification method would suffice. Some felt they could consider delivery by drones with advanced electronic notifications, such as text messaging or emails.

b. Drone package deliveries. A mixture of respondents, although against drone deliveries, felt they would not be giving up on their personal privacy when asked what they thought about cyber/wireless capabilities that could make package deliveries to their residences using drones. One respondent never considered drone deliveries or any risks that could be associated. Six respondents were adamantly opposed to cyber/wireless capabilities of drone package deliveries to their residences. However, in addition to text messaging and emails, one respondent felt advanced phone calls could reduce risks in drone deliveries to residential homes.

Drone Experiences

Survey questions resumed in Tables 17-43 for questions 13-38 to reflect participant responses based on completed open-ended survey questions extracted and analyzed from the online SurveyMonkey tool. Spawned by the three main research questions, questions 13-38 were cyber-related queries about participants' perception of their experiences and knowledge of drones, privacy, and laws. Fourteen participants were forwarded a link to the 39-question online survey using SurveyMonkey.

The group of questions provided key insights into residents' views and perceptions of drones flown in residential areas, which resulted in three areas of concentration related to each of the three research questions. One area captured information about the central phenomenon of participants' perceived drone experiences. Another area focused on participants' perception of their awareness of drone capabilities to gather information. The third area examined information on participants perception of legal actions in the handling of drone situations within residential areas. Except where self-explanatory, each of the following tables describe detailed content analyses derived from participant responses, questions 13-38. The final question, #39, allowed participants to identify how they preferred to be contacted following survey completion, if desired.

Table 17: Question #13 – Drone Knowledge

What do you know about drones?

Respondent Number	Response Text	Content Analysis
6	Very little.	P6, P7, and P11 considered they knew very little about drones or unmanned aerial systems.
7	Very little.	
11	Not much.	
3	I'd say I know a fair amount.	P3, P8, and P13 thought they knew a fair amount of information about drones.
8	Very little other than people fly them and use cameras to scan areas below.	
13	I know they are remote control mini helicopters flying around	
14	They are remote control vehicles.	
1	They are the modern technology for photography, surveillance, and search & rescue	P1, P2, P4, P5, P9, P10, and P12 felt they were quite knowledgeable and understood uses and capabilities of drones and UAS'.
2	They are remote control driven flying apparatus that can carry a small load, and be equipped with electronic devices such as cameras.	
4	They are remotely piloted aircraft that may be used for warfare, aerial photography and recreation/sport.	
5	Price, where to buy, how they function, uses, how they record footage and how they operate	
9	It is a flying robot that is controlled with a device. These robots can observe areas with the use of a camera.	
10	I know that they are used in a wide range of industries, from surveillance or delivering packages.	
12	Minimal information- drones are both used as recreation and for other purposes. Recreation- individuals fly them for entertainment at times with video equipment attached, Other Purposes/Other then recreational- I believe companies fly them, again with cameras, to get pictures to include on maps, internet, etc. Also, companies are wanting to try delivering items utilizing drones, such as Amazon.	

Table 18: Question #14 – Drone Experience

What is your experience with drones flown in any residential area?		
Respondent Number	Response Text	Content Analysis
6	None.	P6, P13, and P14 indicated they had no experience with drones or UAVs.
13	None I have never seen them.	
14	None.	
2	A neighbor has one that a cellular device camera can be affixed and video or photographs can be taken.	P2, P4, P5, and P12 acknowledged one sighting of a drone in neighboring or recreational areas, but no experience.
4	I know a neighbor that has flown his drone in our neighborhood.	
5	Witnessed one flying overhead during a softball game. Other than that very little.	
12	Very minimal- I have only seen one drone flown in my neighborhood, and that was during a holiday when another neighbor was setting off fireworks. I assume someone was wanting a "closer" look.	
1	I see them during firework displays, I feel they should be flown over an open field/rural area rather than in residential areas.	P1, P3, P7, P8, P9, P10, and P11 felt they attained some experience with drones when they witnessed or handled two or more drones. P3 felt quite comfortable with experience gained.
3	The term drone indicates that a UAV or an aerial model is acting on its own to reach a destination or complete a task. It is not legal to fly autonomously in residential areas, that being said my experience flying UAVs or aerial models in residential areas is extensive.	
7	I have witnessed a few recreational drones flown in my area.	
8	I have seen a couple neighbors use them.	
9	I have seen them flown in my neighborhood as well as used for a business to capture images of the current crowd level.	
10	My brother has a drone and he has flown it once or twice in residential areas. I would just stand and observe while he was actually controlling it.	
11	I've seen a few.	

Table 19: Question #15 – Time of Events

What day of the week and time of day have you experienced a drone flying in your neighborhood?

Content Analysis: Ten respondents encountered drones where one or more participants experienced activities in the afternoon and through the night on weekends.

Answer Options	Morning (5:00 a.m. to noon)	Afternoon (noon to 6:00 p.m.)	Evening/Night (after 6:00 p.m.)	Response Count
Sunday	1	5	6	8
Monday	0	1	1	1
Tuesday	0	1	1	1
Wednesday	0	1	1	1
Thursday	0	1	1	1
Friday	0	1	3	3
Saturday	0	5	6	8
			#Answered Question	10
			#Skipped Question	4

Table 20: Question #16 – Internet Connections

Which of the following devices do you most often use to connect to the internet?

Content Analysis: Half of the respondents used their wireless devices (smartphones) to access the Internet.

Answer Options	Response Percent	Response Count
Computer tablet	14.3%	2
Laptop computer	35.7%	5
Smart phone	50.0%	7
	#Answered Question	14

Table 21: Question #17 – Cyber Device Accesses

What do you think about drones entering your private spaces, accessing your cyber/wireless devices, creating data about you, and placing that data in a cloud?

Respondent Number	Response Text	Content Analysis
1	I feel those actions are a violation of my privacy, not in agreement of that.	With the exception of P3, all respondents felt it illegal or a violation of their privacy when drones entered their private spaces, accessed their cyber/wireless devices, created data about them, and placed that data in a cloud; respondents also cringed at the thought of their information collected without their knowledge and placed in some unknown location. Participant #3 responded in an elite manner highly educated in cybersecurity and drones felt protection of cyber devices, privacy, or otherwise, were that of the homeowner.
2	Unless governed by a search and seizure warrant for a criminal investigation- illegal.	
3	Collecting data about my internet-connected devices is nothing new, wardriving has been and still is a very good way to collect intelligence on devices with radios built in. So, in all honesty...so long as the aerial vehicle is being flown carefully and doesn’t endanger my family or property and it is not being done excessively, I don't mind at all. I believe it is up to the owner of any devices with radios to understand how they work and properly protect them. I also do not really believe that any space outside the walls of my house can be considered private, so pictures and other data that can be collected is really my own responsibility.	
4	As long as all of the activities are legal, I am ok with it. I don't think it should be legal for a drone to fly within view of your windows while over your property boundaries.	
5	I'm incredibly nervous about this. Need to rethink how to ensure my network is setup to prevent these types of attacks.	
6	I do not think it should be legal.	
7	This practice makes me a little uneasy. However, if it's for the purpose of public safety I am less bothered.	
8	I was not aware of that, but I don't agree with them doing that.	
9	It is always concerning because you are not aware of who will be able to access that information.	
10	I would be very concerned if this was done without my consent.	
11	Not good - invasion of privacy.	
12	It's unsettling.	
13	Against it.	
14	It makes me uncomfortable.	

Table 22: Question #18 – Visitor Internet Connections

Describe your cybersecurity practices for new Internet or web-enabled cyber/wireless devices entering your residential space (e.g. When a visitor arrives with an internet-ready/WI-FI crockpot for a barbecue or cookout).

Respondent Number	Response Text	Content Analysis
2	None	P2 and P11 indicated they have not had visitors with devices needing connection.
11	Not had this experience	
1	Keep it away from my space/domain	P1 desired to keep these devices off of his controlled domain.
4	We have a WPA secured wireless network. If as user that I trust asks to connect, I give them the password.	P4 through P10, and P12 through P14 practiced cybersecurity of guest connections through pre-shared keys and passwords.
5	I only allow family to access our Wi-Fi network and it's only been laptop, never tablets or smartphones.	
6	Depending on who it is I may give them my password.	
7	I typically give the person my WI-FI password if they are a friend or relative	
8	A allow friends and family to access my WI-FI with my permission	
9	I have not experienced the WI-FI crockpot but have given friends my WI-FI password to access our network. I have not ever given out information to someone that I do not know at my house.	
10	If there is a new device, I make sure I trust the brand. But also, if it’s a friend coming over, I make sure that I'm the one putting in the WI-FI password.	
12	Password needed	
13	Security code	
14	We have a WI-FI password and do not give it out to anyone.	
3	I have separate networks for guests and my own personal devices. Guest devices are not allowed to access anything inside of my trusted network. I don't even allow cable set top boxes to access my trusted network. Trusted devices have their physical addresses modified so as to mask their true function and on capable devices I use a form of PKI for authentication, trusted devices that are not capable each have their own PSK [pre-shared key] for encryption of the radio channel. I also operate false access points and clients to throw off potential sniffers.	P3 segmented networks in trusted domains according to trusted and untrusted users; this permitted an additional layer of network protection for trusted users and cyber devices.

Table 23: Question #19 – Secure Processing

What precautions do you take to securely perform sensitive activities (e.g. banking) when using cyber/wireless devices?

Respondent Number	Response Text	Content Analysis
2	None.	P2 and P6 did not use cyber/wireless devices to perform sensitive activities, such as banking.
6	I do not do them on wireless devices.	
1	Log out of sites, not accepting every cookie, completely turn off computers, tablets, etc.	P1, P3, P4, P5, and P7 through P13 took several precautions to ensure secure transactions over cyber/wireless devices, most commonly was the use of secure encrypted connections to trusted sites.
3	I only use trusted devices that have been properly connected to my trusted network with the best encryption I can use. This doesn't fully protect me though I am aware and I accept the risk.	
4	I don't do banking on a device that I don't trust. Including untrusted WI-FI hotspots.	
5	Ensure that my connection to the sites with sensitive information is always encrypted.	
7	I only do this on my home (locked) WI-FI or on my phone.	
8	Try not to do banking or security type transactions online unless it is with a secure site.	
9	I try not to use my cell phone to access any sites that are more sensitive. I mainly use my computer, which has more protection from others interfering with my information.	
10	I try to limit access my banking to my home WI-FI, which I know is secure. I never connect to any open WI-FI signals and very rarely access my banking account on cellular data.	
11	Use the bank apps.	
12	Multiple passwords, multiple sites, etc.	
13	Security codes	
	#Answered Question	13
	#P14 Skipped Question	1

Table 24: Question #20 – Notification of Unauthorized Events

Who would you call or notify if you suspect unauthorized activity (e.g. unauthorized surveillance or possible electronic ransom) on any of your cyber/wireless devices in your home? Why would you select that person?

Respondent Number	Response Text	Content Analysis
6	Not sure.	P6, P8, P13, and P14 had no idea of whom they would call if they suspected unauthorized activity on their cyber/wireless devices.
8	Not sure	
13	Not sure	
14	I am unsure.	
2	Local police to initiate a possible criminal complaint and then the FBI because local police do not have the resources to investigate such as crime.	P2, P4, P5, P7, P10, and P11 indicated they would contact a law agency, such as the police or FBI, or the Internet Service Provider for suspected unauthorized cyber/wireless activities; although P5 also indicated he had enough knowledge to take care of the problem.
4	The local police. I believe they could advise on whether the activity is legal and provide further contact information if needed.	
5	Other than the police, I wouldn't call anyone else. I have enough Computer/Network experience to handle situations that may arise on my network.	
7	I would contact the local police and possibly my internet provider. The police would be contacted for prosecution and investigation, and my internet provider for preventative measures going forward.	
10	Most likely the police, in order to probably document everything and start an investigation.	
11	??? The wireless company. The cops?	
1	FCC, FAA, they are likely to be conducting the actions.	P1 would contact a federal governing agency, such as FCC or FAA; P3 and P12 would handle the situation themselves; and P9 would alert whoever was affected during the breach and notify the service provider.
3	I wouldn't call anyone; I'd collect as much information as I could about the people performing the surveillance and make a decision based on that information.	
9	If it is my bank or credit cards, I would alert them first. From there I would contact my cable company to alert them because they are the ones who provide the service.	
12	Honestly, I do not know. My husband would handle it.	

Table 25: Question #21 – Remote Provider Actions

What cyber/wireless device and what actions can your provider take to remotely control their device without your permission or knowledge? (For example, your cable provider may send periodic updates to their WI-FI-enabled set top box to provide a new capability or correct a vulnerability)

Respondent Number	Response Text	Content Analysis
5	I am not aware of any.	P5, P6, P7, P9, and P13 were altogether unsure of any action their service providers could take remotely to control their cyber/wireless devices.
6	Not sure.	
7	I am not sure.	
9	I am not exactly sure to what extent they are able to make changes without our consent or knowledge.	
13	Not sure.	
1	Just about all they wanted to do, alarming isn't it?	Respondents P1-P4, P10-P12, and P14 all indicated their service providers could remotely perform updates or some action to their cyber devices without the participants' knowledge.
2	I'm sure any electronic device such as computer or smartphone connected to a server can be hacked remotely.	
3	A set top box can be remotely controlled by a provider and thus they are not trusted devices on my network. I am positive other devices that I consider trusted can also be remotely controlled but I accept that risk.	
4	My cable/internet provider can remotely update our home wireless router or cable box's without our permission.	
10	Most companies send out automatic updates over the cloud (i.e. Apple, Microsoft) this can change everything about your device; performance, storage etc.	
11	Remotely update and reset.	
12	Cable Provider- periodic updates, BGE-monitor/control air/heat levels.	
14	Wireless box.	
	#Answered Question	13
	#P8 Skipped Question	1

Table 26: Question #22 – Recording of Wireless Signals

How concerned are you if a drone has the capability to pickup and record wireless signals from within your residential domain? On a scale from 1 (not) to 5 (extremely), please rate how concerned you are with each device. By concerned, it means the more concerned you are about a device, the higher you would rate it. The less concerned you are about a device, the lower you would rate it.

Content Analysis: Nearly half of the respondents showed extreme concern with drones having the capability to pickup and record wireless signals from their residential domain.

Answer Options	Not applicable	Not concerned	Slightly concerned with no protection.	Moderately concerned with some protection.	Extremely concerned, but adequately protected.	Extremely concerned; do not know what to do, no protection, or no solution.	Rating Average	Response Count
Computer (e.g. laptop, PDA, etc.) connected via wireless network	0	2	0	5	6	1	3.29	14
Mobile phone	0	3	1	4	4	2	3.07	14
Wireless home phone	2	5	2	2	3	0	1.93	14
Wireless Garage Door Opener	0	4	4	3	2	1	2.43	14
GPS	5	3	2	1	3	0	1.57	14
Web-enabled appliance (e.g. refrigerator, air conditioner/thermostat, microwave, television)	5	4	1	2	2	0	1.43	14

Table 27: Question #23 – Legal Measures

What legal measures do you envision can be implemented to block or jam unwanted drones from capturing wireless signals from your residence?

Respondent Number	Response Text	Content Analysis
6	Not sure.	P6, P8, P11, P12, and P13 felt they could offer any idea on blocking or jamming of undesirable drones from capturing wireless signals.
8	No idea	
11	?	
12	Not sure.	
13	Not sure.	
1	Other than shutting down and unplugging devices, not much, government infused program.	P1 considered a system shutdown to appropriately block the activity.
2	Marketed jamming devices and can emit a signal to block/jam external devices from capturing internal signals.	P2 and P14 shared a direct technological solution by jamming.
14	Using a long-distance jammer.	
3	No measure can stop the collection of radio signals emanating from my residence.	P3 indicated collection wireless signals from residential areas couldn't be stopped.
4	Encryption on all sensitive transmissions and devices.	P4 offered an encryption solution to ward off the unwanted capture of wireless signals.
5	Heavy fines and possible jail time.	P5 felt fines and jail time could be a deterrent to unwanted capture of wireless signals.
7	I am not sure. Restricted air space perhaps.	P7 indicated handling of unwanted capture of wireless signals could be through policy.
9	It would all depend on your Terms of Service with the companies that you have your cable, electric etc. Many of them must use wireless and would state what will be done to cover themselves.	P8 noted the handling was dependent on service provider-defined terms on their policy to address unwanted capture of wireless signals.
10	Routers would somehow need to constrict the signal. But you could have security cameras that allow to see the drone, but that doesn't stop the drone per say.	P10 offered a technological approach through monitoring since it was noted such wireless capture could not be prevented.

Table 28: Question #24 – Drones and Package Deliveries

What do you think about cyber/wireless capabilities to make package deliveries to your residence using drones? (It has been recently reported that drones are being used to deliver in difficult to reach locations.)

Respondent Number	Response Text	Content Analysis
1	That is totally crap and should be ruled unconstitutional; a total invasion of privacy	P1, P5, P6, P8, P13, and P14 were adamantly opposed to cyber/wireless capabilities for drone package deliveries to residences.
5	Very much opposed to this with the exception of using it for medical emergencies.	
6	I do not think that this is a good idea.	
8	Would prefer that not be the option used	
13	Not good.	
14	I do not like that idea because it takes jobs away from people.	
2	Raises possible threat to commercial aircraft, especially since reside near a major airport.	P2, P3, P4, P7, P9, P10, and P12 were very open and receptive to the concept using cyber/wireless technology to deliver packages by drones.
3	I think if they have the proper safety procedures in place, they could be an absolute revolution to how delivery works in our world.	
4	I think it can be a good idea if it's affordable	
7	I don't see any issue with this.	
9	I don’t see this as an issue in our area because of being so close to the airport.	
10	I think this is an okay idea, but it could easily bad (i.e. people shooting down drones, drones losing signal, etc.)	
12	I am open to it; however, I feel it still needs to go through a multitude of tests firsts to determine how effective, safe and accurate it is.	
11	No thought about it	P11 never considered drones to deliver packages.

Table 29: Question #25 – Notification of Drone Deliveries

What notification methods would allow you to feel wireless deliveries by drones to your home are acceptable (e.g. phone calls or text messages made with at least a day’s notice)?

Respondent Number	Response Text	Content Analysis
1	None whatsoever	P1, P6, P13, and P14 were against deliveries by drones.
6	None.	
13	None	
14	None	
5	Phone Calls	Although P5 was opposed to deliveries by drones, phone calls could be acceptable if drones made deliveries.
2	Email or text to preregistered device would be sufficient.	P2, P3, P4, and P7 through P12 thought electronic notifications through text messages or email were acceptable means prior to deliveries by drones.
3	An e-mail is fine.	
4	An email or phone call within a day of delivery would be acceptable.	
7	Text message or email	
8	Email	
9	Email or text would be fine.	
10	Yes, a heads up would be nice, so you don't mistake the drone as an attack or something of that sort. The delivery service should notify users based on their preferences.	
11	Text messages	
12	Text messages and/or emails	

Table 30: Question #26 – Privacy versus Delivery

What are your thoughts about drone deliveries to your residence and giving up on your privacy to have such a wireless delivery made?

Respondent		
Number	Response Text	Content Analysis
1	It's bull crap and should not be implemented.	P1, P5, P6, P9, and P13 indicated they were totally against drone deliveries to their residences and thought it a bad idea when privacy was jeopardized.
5	Very much opposed to this.	
6	I would not want them.	
8	Prefer that option not be used.	
9	I do not need drone deliveries and do not think they would benefit in any way.	
13	Don't like.	
2	No difference than if a courier placed it at the residence.	P2, P3, P4, P7, P10, P11, and P12 seemed to be acceptable to the idea of the possibility of giving up on privacy for the capability to have drones deliver packages.
3	Not sure I am giving up any privacy by allowing that to happen. The same data can be collected by a delivery person with a sniffer in their pocket.	
4	It's ok as long as certain rules are followed (no cameras pointed into windows, etc.).	
7	This doesn't bother me.	
10	It really depends what data the drone collects, if it simply makes a delivery and then takes a picture of the package (not the house) that would not be as big of a concern to me.	
11	Depends on the vendor.	
12	I feel it's very similar to online shopping.	
	#Answered Question	13
	#P14 Skipped Question	1

Table 31: Question #27 – Local Cybersecurity Policies

What local cybersecurity/wireless policies are you aware of that regulate the flying of drones in private areas, such as around your home?

Respondent Number	Response Text	Content Analysis
4	I'm not aware of any drone specific cyber polices.	P4 through P7, and P10 through P14 were not aware of any Anne Arundel County or local cybersecurity or wireless policy that regulated the flying of drones in residential areas.
5	None that I am aware of.	
6	I don't think there are any.	
7	I am not aware of any policies	
10	I'm not aware of any local policies in residential areas	
11	?	
12	None that I know of.	
13	None.	
14	None.	
1	Must have a registration number physically placed on each drone, not to fly within 5 miles of an airport, although I think that has been modified (lifted).	P1 and P2 noted their knowledge of drone registration requirements and flight restrictions, but did not state they were aware of any Anne Arundel County or local cybersecurity or wireless policies that regulated flying of drones in residential areas.
2	Laws that prohibit drone height and registration.	
3	I live close to an airport and the FAA restricts the height of aerial models and UAVs other than that I am allowed to fly using caution as I see fit. If a neighbor of mine had a problem with me flying I'd respect that but I'd ask that they also make themselves aware of the laws.	P3, P8, and P9 noted their knowledge of no-fly zones around airports, but did not state they were aware of any Anne Arundel County or local cybersecurity or wireless policies that regulated flying of drones in residential areas.
8	All I know is that there are certain "no fly" spaces that drones are not supposed to enter.	
9	I know the FAA has some guidelines in place but I am not exactly sure. I also know that they are still making changes as to what drones can fly over, by etc.	

Table 32: Question #28 – State Cybersecurity Policies

What state cybersecurity/wireless policies are you aware of that regulate the flying of drones in private areas, such as around your home?

Respondent Number	Response Text	Content Analysis
1	Not aware of much.	P1, P3 through P8, and P10 through P14 were not aware of any Maryland cybersecurity or wireless policy that regulated the flying of drones in residential areas.
3	Again I don't consider the airspace above or around my home any more privileged then that of my neighbors. I am not aware of any legal distinctions.	
4	I'm not aware of any drone specific cyber polices.	
5	None that I am aware of.	
6	I don't think there are any.	
7	I am not aware of any policies.	
8	Not aware of any.	
10	I'm not aware of any state policies in residential areas.	
11	?	
12	None that I know of.	
13	None.	
14	None.	
2	They are required to be registered and have height restrictions.	P2 and P9 noted their knowledge of drone registration requirements and flight restrictions, but did not state they were aware of any Maryland cybersecurity or wireless policies that regulated flying of drones in residential areas.
9	I know the FAA has some guidelines in place but I am not exactly sure. I also know that they are still making changes as to what drones can fly over, by etc.	

Table 33: Question #29 – Federal Cybersecurity Policies

What federal cybersecurity/wireless policies are you aware of that regulate the flying of drones in private areas, such as around your home?

Respondent Number	Response Text	Content Analysis
2	Not sure.	P2, P4 through P8, and P12 through P14 were not aware of any federal cybersecurity or wireless policy that regulated the flying of drones in residential areas.
4	I'm not aware of any drone specific cyber polices.	
5	None that I am aware of.	
6	I don't think there are any.	
7	I am not aware of any policies.	
8	Not aware of any.	
12	None that I know of.	
13	None.	
14	None.	
1	Registration numbers physically displayed on each drone.	P1, P3, P9, P10, and P11 noted their knowledge of drone registration requirements or flight restrictions (e.g. void from airports) and knew there were federal regulations. P3 mentioned an FAA article identified operational limits for UAS', however, the article did not state it regulated flying of drones in residential areas.
3	I am registered to fly and I adhere to the rules set forth by the FAA, https://www.faa.gov/uas/media/Part_107_Summary.pdf.	
9	I know the FAA has some guidelines in place but I am not exactly sure. I also know that they are still making changes as to what drones can fly over, by etc.	
10	I do know that your drone has to be register with the FAA, and you can't fly near airports are certain heights. (Not sure if this is federal level.)	
11	Can't fly drones close to an airport.	

Table 34: Question #30 – Residential Wireless Policies

What other kind of wireless policy can be implemented to ensure web-enabled cyber devices are not intruded when there is a drone flying around your home?

Respondent Number	Response Text	Content Analysis
5	Unsure.	P5, P6, P8, P11, P13, and P14 were not sure if there could be any wireless policy that could be implemented to ensure web-enabled cyber devices were not intruded when there was a drone flying around their homes.
6	Not sure.	
8	Not aware of any	
11	?	
13	Not sure.	
14	I am unsure.	
3	Nothing, wireless digital communication is enabled by radio transmission, and anyone who believes that those signals are private in any way shape or form are wrong. You can protect yourself by either not using those devices or using those devices in such a way as to deter the collection of the signals.	P3 felt nothing could be implemented to ensure web-enabled cyber devices were not intruded when there was a drone flying around his home.
1	Keep them at a certain minimum (higher) altitude and flying time restrictions	P1, P2, P4, P7, P9, P10, and P12 shared a number of controls and solutions they felt could be implemented to secure web-enabled cyber devices from drones flying around their homes: • Altitude restrictions • Time of flight restrictions • Distance from home restrictions • Laws and policies to protect privacy from drones • Some form of jamming device • Encryption of personal traffic
2	Other than making laws that make such an action illegal, only a jamming device can block or deter the action.	
4	All wireless policies applying to other vehicles/pedestrians should apply to drones.	
7	Approval links sent to homeowner.	
9	Drones should have to be registered and from what I am aware of I don't think that is the case anymore.	
10	Make sure that the drone cannot access the network at all. If it can access it make sure the traffic is encrypted so the drone is not taking any real information.	
12	I would like to know that there is a certain number of feet the drone would have to be away from my house, a law about not recording/taking pictures of my house or people on my property, and somehow know there is a way to protect the information my family has on the Internet, or in the cloud, etc. (All of these items could exist, and I just may not be aware of them.)	

Table 35: Question #31 – Law Enforcement of Drone Activities

What do you know about law enforcement's handling of drones flown in residential areas?

Respondent Number	Response Text	Content Analysis
1	Nothing, not sure if the local law enforcement have much concern over drones	The majority of respondents (P1, P3, P4, P6 through P9, and P11 through P13) overwhelming felt they knew of nothing could be done to address law enforcement's handling of drones flown in residential areas.
3	Nothing, I am not aware of our local police using devices like that for aerial reconnaissance.	
4	Nothing.	
6	I do not think that they can do anything.	
7	I am not aware of law enforcements policies.	
8	I am not aware of any of these situations and how they should be handled.	
9	I do not know how this is handled.	
11	Nothing.	
12	Nothing.	
13	None.	
2	None. However, it would be a useful tool to use for surveillance in difficult to reach locations that would otherwise compromise an investigation. However, I'm sure laws or procedural ordinances would govern its use.	P2 indicated drone use could be useful in surveillance and thought there could be laws to address law enforcement's handling of drones flown in residential areas.
5	From my understanding, law enforcement is very restricted in how it can handle drones. There is not a lot being done to stop them.	P5 indicated there were restrictions, but did not state what restrictions and felt little could be done to address law enforcement's handling of drones flown in residential areas.
10	I know that in certain areas law enforcement has shot down drones. As for residential areas, I have not heard anything. But I'm sure they would be able to stop any drones if need be.	P10 indicated drones had been shot down by law enforcement, but did not state where or when; also, P10 felt something could be done to stop drones, but did not state what.
	#Answered Question	13
	#P14 Skipped Question	1

Table 36: Question #32 – Home Security versus Drone Operations

Using a scale of 1-5, 5 being the most invasive, how would you rate drone operations in residential areas and why? By invasive, it means how threatened you think you feel by a drone flying over or near your home with the possibility of receiving wireless signals from your home cyber devices.

Respondent Number	Response Text	Content Analysis
1	5, dishonest people can purchase drones for neighborhood surveillance, i.e., monitor times of least inactivity of residents	There were 35.7% of respondents who indicated *5* and felt drones in their residential neighborhood was most invasive, 14.3% rated *4-4.5*, 21.4% rated *3*, 14.3% rated *2*, and 14.3% rated *1*.
2	4	
3	1	
4	2. I don't feel its much more invasive than a vehicle driving by. I expect that I am responsible for securing wireless networks adequately.	
5	5	
6	5. I feel it is an invasion of privacy.	
7	2	
8	3	
9	3	
10	4.5, depends on the operation really	
11	3	
12	1- because it is not a problem in my neighborhood	
13	5 I don't like my privacy being affected	
14	5	

Table 37: Question #33 – Residential No-Drone Policy

How could a no-drone-zone policy for drones be applied to residential areas? (FAA created a No-drone-policy around airports and hobbyists can fly their marked and registered, under 55 lb. drone no higher than 400 feet, but must contact airport officials if within (5) miles of an airport.)

Respondent Number	Response Text	Content Analysis
6	Not sure.	P6, P11, and P12 were unsure of how a no-drone-zone policy for drones could be applied to residential areas.
11	?	
12	Not sure	
1	Implement a no-drone-zone policy for all residential areas other than an open park/field, or undeveloped areas	P1 and P7 felt a no-drone-zone policy could be applied to residential areas, but did not state how.
7	A no fly policy seems reasonable.	
2	Laws can be created, but enforcement becomes an issue.	P2 and P8 felt even if there was a no-drone-zone policy for drones in residential areas, it would be difficult to enforce.
8	Who would enforce this? The residents of the neighborhood?	
3	Jammers are the only thing I can think of, but that's a very bad way to enforce a policy like that. People being aware of the laws and properly reporting are the best defense in my opinion.	P3 felt that jammers could be applied in a no-drone-zone policy for drones in residential areas, but also felt defensive mechanisms could really be the best defense.
4	Perhaps a drone should be restricted to no lower than 100 feet when passing a private property boundary unless having the owner's permission.	P4 felt gaining an owner’s permission could be applied in a no-drone-zone policy for drones in residential areas.
5	Homeowners/Neighbors would need to be notified and approve of drone fly overs, otherwise it should be considered illegal	P5 felt neighborly notifications and approvals must be obtained; otherwise, it would be a no-drone-zone policy for drones in residential areas.
9	Similar as the airport.	P9 felt no-drone-zone policies for drones could be applied to residential areas as are at airports.
10	I think creating a map (integrated into the drone app) that would show no fly zones. To which, residents can add their homes if they would like.	P10 felt a technological solution that integrated residential homes into the drone application could be used to distinguish the homes as a no-drone-zone.
13	Not sure maybe a petition.	P13 felt a petition could be made to address a no-drone-zone policy for drones in residential areas.
	#Answered Question	13
	#P14 Skipped Question	1

Table 38: Question #34 – Drone Fines

What would you consider to be a reasonable fine to impose on operators when their drone attempts to connect to residential cyber/wireless devices?

Respondent Number	Response Text	Content Analysis
3	If you could determine that with any accuracy I think there shouldn't be any fine. The operator of the access point is responsible for protecting their devices.	P3 and P8 indicated no fines should be imposed on operators when their drone attempted to connect to residential cyber/wireless devices.
8	?	
10	A good amount, maybe around $300 for the second offense.	P1, P2, P4, P5, P6, P7, and P9 through P14 indicated fines ranging from $300-$25,000 should be imposed on operators when their drone attempted to connect to residential cyber/wireless devices.
6	$500.	
9	$500.	
13	$500.	
2	At a minimum- $1000. But seizure of the drone and attached equipment should also be conducted.	
7	$1000.	
1	$10,000 fine, loss of drone capability, and/or a minimum (3 day) jail term.	
4	Should match fines for non-drone activities.	
5	$5000 and up.	
11	$25,000.	
12	I would suggest a first offense, second offense, third offense, type of a fine/consequence.	
14	Yes.	

Table 39: Question #35 – HOA and Drones

How does your homeowner's association address drones flown in your neighborhood?

Answer Options	Response Percent	Response Count
Not applicable, no HOA.	0.0%	0
HOA does not address drones.	92.9%	13
Other (please specify)	14.3%	2

Table 40: Question #36 – Addressing Drones in HOAs

How could a homeowner's association address flying drones to connect to residential cyber devices within your neighborhood?

Respondent Number	Response Text	Content Analysis
1 4 10	Get with the local authorities and ban those actions. I don't think an HOA is a reasonable authority in this area. If a connection is purposely made with harmful intent then I think law enforcement should be involved.	P1, P4, and P10 felt law enforcement or another local authority and not a homeowner’s association should address the flying of drones and any attempt to connect to residential cyber devices within residential neighborhoods.
2 3 5 9	They can add it to bylaws, but enforcement remains the issue. They could create a policy, but that's about it. Enforcement and proper evidence collection would be very hard. I don't think they can. I don’t think they could control that.	P2, P3, P5, and P9 thought enforcement would be an issue even if homeowner associations addressed flying drones to connect to residential cyber devices within residential neighborhoods.
6 8 11 12 13	Not sure. Hasn't been discussed. ? Has not been an issue. Don't know. Not sure.	P6, P8, P11, P12, and P13 noted they were unsure, there had never been an issue, or the subject had never been brought up at their homeowner's association to address flying drones in their neighborhood.
7 14	Create a policy to permit or restrict this activity, as approved by the homeowners. Have discussion about it.	P7 and P14 seemed to think the homeowner’s association should discuss addressing flying drones to connect to residential cyber devices within their neighborhood.

Table 41: Question #37 – Cybersecurity Training

What kind of cybersecurity training do you feel is needed for residences to become more knowledgeable of wireless connectivity capabilities with drones flying in residential neighborhoods?

Respondent Number	Response Text	Content Analysis
6	Not sure.	P6, P8, and P13 were unsure of training deficiencies in cybersecurity in their neighborhood.
8	?	
13	Not sure.	
1	Review the guidelines of the FAA, request quarterly newsletters with regards to updated vulnerabilities of cyber-security effects	P1 through P5, P7, P9 through P12, and P14 desired some form of announcements, notices, education and awareness, informative meetings, and training were needed for residences to become more knowledgeable of wireless connectivity capabilities with drones flying in residential neighborhoods.
2	Public safety announcements, publicize newly enacted laws.	
3	Any and all training necessary to properly educate them on the safe usage of radio systems for digital communications.	
4	Learn how to secure wireless communications and learn whether communications are encrypted and to what level.	
5	Training to ensure all homes networks are secured with the latest encryption methods	
7	Learning how to know if a drone has accessed your home network or devices	
9	I think training would be great but not feasible due to time and money constraints. If there was training it would need to be set up at a local library etc. to help inform the people.	
10	I think it's important to understand the information the can be passed through wireless signals, this may also help implement new laws if needed.	
11	Would be good to have a information meeting	
12	I would need basic, from the beginning. I am sure not everyone would need that, so maybe a differentiated approach based on individual needs.	
14	Some sort of basic training just to bring knowledge to our community.	

Table 42: Question #38 – Expectation of Study Results

What would you expect from the results of this study?

Respondent Number	Response Text	Content Analysis
1	Updated material from the FAA, FCC, local law enforcement implementation, and anonymous reporting procedures.	P1, P2, P5, and P6 indicated they wanted law changes, anonymous reporting, and penalties as a result of this study.
2	Awareness to lawmakers or driving researchers to make additional research.	
5	I think this is an important study. I would hope the results would help lead to stricter laws and penalties potentially for people who use drones to fly over residences and attempt to perform a hack.	
6	Stronger laws governing the use of drones.	
3	Just to be able to read the final product.	P3 desired to read the dissertation once available.
4	A large variety of opinions.	P4 thought the study could produce a great deal of opinions.
7	Further understanding the risks and public sentiment regarding drones, and how often they access personal networks or devices.	P7, P9, P10, and P14 indicated the result of this study should produce more education on security risks with drones and capabilities could access personal wireless and cyber devices, and about risks and mitigations in cybersecurity.
9	That people are not as aware as they should be when it comes to cyber security.	
10	I would say most people don't understand the full extent of what drones are capable, but most people would say that they are invasive.	
14	To learn the basics about cyber security and drones.	
8	?	P8, P11, and P13 were not sure of their desire as a result of this study.
11	?	
13	Not sure.	
	#Answered Question	13
	#P12 Skipped Question	1

Table 43: Question #39 – Future Contact Method

How would you like to be contacted once the survey is complete and available for release?

Answer Options	Response Percent	Response Count
No follow-up desired.	21.4%	3
Please use the same email method.	71.4%	10
Other (please specify, e.g. call (800) 555-1212))	7.1%	1
	#Answered Question	14

Summary

Chapter 4 presented details reflected of 14 study participants' responses to online surveys on how private citizens perceived privacy when drones flown over their residences could possibly access cyber devices operating within their homes. The SurveyMonkey instrument allowed the design, administration, distribution, collection, and analysis of 39 survey questions. Data extrapolation supported reassembly of data into many forms of usable information presented in various tables and charts.

Four major themes materialized from analytical data drawn from 14 respondents', which further evolved from the 39 elements of an online survey. The resulting themes were: (a) cybersecurity practices; (b) laws, policies, law enforcement, fines, notifications, and reporting; (c) residential education in cybersecurity; and (d) package deliveries by drones. Chapter 5 discusses study limitations, interpretative findings, and recommendations to address gaps found from the literature review and as identified by research results.

CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS

Thousands of drones sold for recreational purposes present substantial challenges, such as the ability of drones to connect to wireless links, in residential areas where drones equipped with cameras could be used for unlawful viewing and data collection of a person’s private property (Choi-Fitzpatrick, 2014). Consequently, technological growth and residential education of cybersecurity nuances, strengths, weaknesses, challenges, and defensive mechanisms and approaches create a larger number of unanswered questions. Gaps were found to exist in current information following the literature review of drone capabilities could allow an invasion of a person’s privacy through the use of drone technologies. A survey of specialized questions (APPENDIX C) was created and distributed to participants before semi-structured interviews were held, which allowed amplified participant responses based on perceptions of cyber devices accessed by drones.

The specific problem was residents lacked understanding of the laws and regulations regarding the right to privacy regarding drones, which could be used to violate those privacy rights. The study looked at what residents understood in their right to privacy or what constituted an invasion of privacy in their perception of drones operating over residential areas. Although FAA Modernization and Reform Act of 2012 is a federal document, it does not currently apply to residential or local areas; however, it could be a pillar to address residential legal needs for spaces that are continuously questionable as reasonable private areas. Jacobstein (2013) noted residents might not be educated on vulnerabilities associated with data collection gained from drones that could lead to inappropriate data sharing of personal information.

The purpose of this qualitative phenomenological research was to understand how private citizens perceived privacy when drones flown over their residences could access cyber devices operating within their homes. The research stayed on track using a sound research approach focused on the research question, “what perceived privacy rights are associated with private, individual use of drones operated in a Maryland residential area?” The research method consisted of a qualitative phenomenological approach that allowed the gathering of information on adult residential citizens regarding their perceived expectations of privacy related to drones. Erkip and Mugan (2010) indicated a qualitative research approach was most appropriate when gaps exist in the literature surrounding a study.

This qualitative research was structured through the exploration of studies, interviews, document examinations, and participant queries contributed to the phenomenological insights gained from individual experiences as suggested by Akkoyunlu and Daghan (2014). Several data analysis tools were used to analyze data collected from participating respondents and study interviewees. The online SurveyMonkey questionnaire and analysis tool permitted organization, development, distribution, and management in the singular and self-evident content analysis of participant survey questions (APPENDIX C) and interviews. Chapter 5 includes details on limitations, summary of findings, interpretation of findings, researcher recommendations, and recommendations for future research.

Limitations

Limitations inherent to this qualitative phenomenological study included: (a) number of study participants, (b) participant understanding, (c) time constraints, and (d) a lack of applicable Maryland law and policies on drones and privacy. Although the goal was to study 18 adults, resident availability was a limitation and therefore, research size reflected 14 study participants. Identification of respondent’s level of education carried study limitations noted after participants initiated the survey and certain technological references presented limited understanding.

Cassell and Symon (2011) noted there was no need to expend additional time during a qualitative research because of difficulties to seek alternative criteria. Time constraints to review and coordinate were only limited by the inability to extend the survey to other residential neighborhoods, even though the intent was the singular targeted Linthicum Heights neighborhood. Participants were quickly identified through an already established email group and communications were easily tracked. Although drone sightings were noted around the Maryland neighborhood, no research biases were identified; however, Florida law was referenced due to the lack of applicable Maryland policies on drones and privacy.

Summary of Findings

The purpose of this qualitative phenomenological research was to understand how private citizens perceived privacy when drones flown over their residences could access cyber devices operating within their homes. The study was driven by three guiding research questions:

- How do residents feel if faced with a drone flying within their residential private spaces and accessing their cyber devices?
- How do residents feel about drones entering their private spaces, collecting data about them, and placing that data in the cloud?
- How do residents feel regarding law enforcement’s handling of drones flown in residential areas?

Survey analyses revealed a very high desire to learn more about drones and the dangers of wireless and cyber devices in residential areas. Participants indicated a need to use better defensive tactics and identify where weaknesses lied in their personal domains. Also, residents had mixed feelings on establishing local drone laws because of how difficult it was to distinguish what a violation was, policies not already established, or the trouble it may be just to enforce a policy if there was a violation.

Interpretation of Findings

Theme 1: Cybersecurity practices

Although cybersecurity, cybersecurity practices, and technological implementations weighed high on all participants, only six of the 14 respondents took precautionary measures in their cybersecurity practices for new Internet or web-enabled cyber/wireless devices, such as the Internet of Things (IoT). Lack of cybersecurity practices could have been due to participants' technological unfamiliarity to protect their privacy. Additionally, participants could have had a level of uncertainty to identify possible flaws that existed in their network environment or they may not have possessed enough awareness to implement good security practices during sensitive activities, such as online banking.

A Public Service Announcement made by the Federal Bureau of Investigation (FBI) warned of the IoT where a device could automatically connect to the Internet. Further, IoT devices could transmit or even receive emitting data, as homeowners become targets for such malicious or rogue acts and fall victim to eavesdropping and exploitation (FBI, 2015). FBI (2015) indicated IoT devices such as heating/air conditioners, Wi-Fi systems (including computer networks, security systems, and baby monitors), lights, peripherals, and even home entertainment systems reaped opportunities for exploitation because of weak or nonexistent security measures. Oddly as it sounds, wearable fitness devices were also among the list of IoT items susceptible to exploitation (FBI, 2015). A no-drone-zone policy could help decrease residences uneasiness of their information being targeted from a drone or their feeling of an invasion of privacy; however, cyber threats remain and continuous cybersecurity training is still needed for residences to be made more knowledgeable of wireless connectivity capabilities by drones or through any cyber means because of the IoT.

Residents felt there were challenges with a lack of knowledge of cybersecurity, not enough or improper cybersecurity practices, and that they were not up-to-date on technological implementations with drones flying within their residential private spaces and accessing their cyber devices. Residents felt uneasy about drones entering their private spaces, collecting data about them, and the capability to have their data placed in the cloud. Additionally, residents felt cybersecurity practices could be improved by better understanding law enforcement’s role in handling drones flown in residential areas could help protect the residents’ privacy.

Theme 2: Laws, policies, law enforcement, fines, notifications, and reporting

Participants indicated there was a lack of understanding if or what cybersecurity policies existed about drones and privacy. They felt laws, policies, notifications, and reporting existed for airports, but was not sure what to do if faced with a drone flown within their residential private spaces and gained access to their cyber devices. Residents felt there could be laws in those instances to gauge law enforcement’s handling of drones flown in residential areas. Participants thought laws and policies should reflect fines that could be imposed on violators and policies to include stipulations for law enforcement handling, response, and enforcement of those policies. Participants indicated a desire for mandatory public notifications are provided to affected residences and service providers obtain authorizations and permissions for remote access to residential cyber devices.

Residents felt drones entering their private spaces, collecting data about them, and placing that data in the cloud should be controlled. Consequently, there is a need to develop residential cybersecurity policies, define laws, identify ways to enforce those laws, and a means to apply associated fines when those laws are broken. Continuous residential cybersecurity notifications are needed along with a requirement to grant permissions prior to drone activities in residential neighborhoods. Policies to address privacy, remote access, and reporting are also needed for residential areas. Participants noted a reporting system could be put in-place when a resident felt threatened by drones regarding their privacy. As of this writing, there were no known policies to regulate drone activities in residential areas; however, Aquino-Segarra (2016) noted, Federal Aviation Administration regulated drones near or in-flight airspace and operations, not in residential areas.

Theme 3: Residential education in cybersecurity

Cybersecurity training, education, and awareness also resonated highly with respondents who were very straightforward to note their deficiency in understanding wireless vulnerabilities. Residents felt there was national, state, and local work needed to educate users what they could do to protect their networks and information when faced with a drone flying within their residential private spaces and trying to gain access to their cyber devices. Residents also felt there was a need for educational cybersecurity information to be created and distributed about drones entering private spaces with the possibility of collecting data about the residents and placing that data in the cloud.

Residents felt they had no or little educational knowledge regarding law enforcement’s handling of drones flown in residential areas. Information on cybersecurity, cybersecurity practices, and technological implementations could assist residents in management and monitoring of their IoT devices. Awareness could also be made in the form of neighborly notices of planned drone operations by hobbyists to inform residents of nonintrusive devices or to advise them of actions that could help protect their cyber devices. An IoT public service announcement (FBI, 2015) was provided via email to participants who indicated a desire for more information.

Educational levels of participants were used as input into demographics during the survey and as an observation to whether there were any influences on the participants' decision whether to participate in the research or not. Vilalta (2012) found educational differences among lower-educated audiences where there were noticeable impacts in participants' expectations and who expressed vulnerability, as well as, a greater fear of crime. Querying the knowledge level of participants addressed the study purpose, which was to identify perceived expectations of privacy that addressed private, individual drone operations in a Maryland residential area.

Terwilliger (2013) asserted research and development used in UAS situations for academic influence could showcase innovation and creativity, and promote unity in academic excellence among the public community and policymakers on UAS issues. Identifying policies on drone operations in residential areas helped identify some of the policy gaps and revealed allowances or restrictions on actions residents could possibly take when faced with a drone in their reasonably expected private areas (Terwilliger, 2013). Similarly, educational awareness was an area that required modernization to increase acceptance or decrease disregard to a policy or law, as noted by Wolper (2012). With political and financial backing, investments into educational systems could prove quite beneficial to UAS developments and a return on investment for taxpayers (Terwilliger, 2013; Wolper, 2012).

Theme 4: Package deliveries by drones

Delivery notifications and drone package deliveries were services that many respondents felt were worthy of chancing their privacy in order to gain advantage of new technology. Precipitous possession and use of drones continued to be of interest to more than the casual hobbyist with numerous study participants indicating their openness to receiving packages by drones. Reports of deliveries by drones are not new and have included tests of medical and food deliveries, e.g. burritos, to residential and business areas (Stevens & Wells, 2016).

Whether drones were to be used for commercial or private deliveries, some residents felt there could be an invasion of privacy and that form of uneasiness or fear could evidently result in drastic measures taken, such that the drone could be knocked or shot down. Residents felt access to cyber devices and privacy could be compromised if faced with a drone flying within their residential private spaces to deliver packages and that there was no legal mechanism to engage law enforcement in the handling of drones flown in residential areas. A news report noted lawmakers have asked if someone could shoot a drone down when its flying over that person's property; unfortunately, the question went unanswered (Subbaraman, 2013). It was shared during a 2015 hacker conference drones could be used to penetrate computer networks with no or poor security protection (Atherton, 2015).

Researcher Recommendations

Table 44 summarizes recommendations from study results and thematic findings as interpreted by the researcher based on electronic data and personal interviews with study participants.

Table 44: Recommendations

THEME NUMBER	THEME TITLE	RECOMMENDATIONS
1	Cybersecurity practices	1. Understand devices capable of emitting wireless signals and radio frequencies in residential areas.
2	Laws, policies, law enforcement, fines, notifications, and reporting	1. Identify deficient federal, state, and local laws to regulate cyber domains and cybersecurity for residential areas. 2. Establish a forum to allow community collaborations that could create needed residential cybersecurity laws. 3. Identify and define restrictions, stipulate what constitutes violations, and ensure laws created can be enforced.
3	Residential education in cybersecurity	1. Promote ongoing residential education through local HOAs, media, bulletins, and public announcements. 2. Offer complimentary basic cybersecurity training of a typical wireless network infrastructure.
4	Package deliveries by drones	1. Identify residential restrictions and limitations for drones. 2. Know and arrange a preselected date and time for delivery. 3. Utilize a surveillance camera to monitor internal and external home activities.

Theme 1: Cybersecurity practices

There is a necessity to understand wireless/cyber device risks and protective measures that could be implemented throughout residential homes, as well as, the need to understand the capability of devices emitting wireless signals from cyber devices under a residences' control (this should include knowledge of radio frequencies). For instance, Hutchins and McNeil (2015) indicated wearable devices were among culprits of wireless developments susceptible to a breach of privacy as information was collected about the wearer and processed over the air. DHS (n.d.) has become intricately involved in efforts to supply Americans with information on cybersecurity best practices in residential areas, including tips on immediate actions to take for cyber incidents experienced when at home, work, or in a public location. Recommend residents gain a better understanding of devices capable of emitting wireless signals and radio frequencies in residential areas that could potentially jeopardize their privacy.

Theme 2: Laws, policies, law enforcement, fines, notifications, and reporting

Based on the findings, using drones to possibly access wireless/cyber devices within a residence to probe, collect, or manipulate data and invade privacy remain a major concern. Aquino-Segarra (2016) noted FAA's regulation of drones near or in-flight airspace and operations did not address residential regulatory needs of private citizens' privacy; policies still lag behind in state laws. Recommendations include: (1) Identify deficient federal, state, and local laws to regulate cyber domains and cybersecurity for residential areas; (2) Establish a forum that supports community collaboration to create needed residential cybersecurity laws and bi-laws; and (3) Identify residential restrictions, what constitutes violations, establish minimum and maximum fines, and ensure laws created can be reasonably enforced.

Theme 3: Residential education in cybersecurity

Understanding of IoT could be very complex. Cybersecurity training, education, and awareness also resonate highly among respondents who were very straightforward to note their deficiency in wireless vulnerabilities, advocating a need for better training. Manufacturers, utility companies, and communication suppliers are among those who could provide proper notifications on the kinds of signals, vulnerabilities, and mitigations that apply to their wireless cyber devices. Voas (NIST SP 800-183, 2016) described IoT under the confines of *network of things* (another technological concept not discussed in this writing), which could be a great addition to the educational repertoire on IoT. Recommend improving residential education through local HOAs, media, bulletins, and public announcements could help communities establish initial and rotational monitoring. Further offering of complimentary basic cybersecurity training could help residences understand security needs for a typical wireless network infrastructure.

Theme 4: Package deliveries by drones

If package deliveries by drones come to fruition to a local neighborhood, such as Linthicum Heights, there should be a mandate for those who opt-in, but only with specific delivery notifications. Identification of restrictions and limitations for drones provide residential users the opportunity to implant defensive and protective mechanisms, technologically or administratively. Residents and their guests should know what is expected and when through prearranged dates and delivery times. Also, a surveillance system could be used to monitor home activities inside and out of the immediate residential home.

Recommendations for Future Research

FAA Modernization and Reform Act of 2012 and other uprising federal efforts address safety and security of airspace in flight operations, flight lines, airports, and with non-hobbyists; however, as of this writing, there were no national laws established to set legal measures for flying drones in residential areas where instances of an invasion of privacy could occur. Based on participant responses, there is an overwhelming need to establish laws to protect private residential domains containing cyber devices and to gauge allowances and restrictions of casual drone hobbyists in residential areas. In what seemed to be one-sided protection of federal air spaces, there is a notable void of legal protection of air spaces over reasonably expected private areas.

What about the safety and security of residents who become victims to drones and UAS' crashing into their property, intercepting their data, or that invade their privacy? Where are the cops to patrol residential areas and spaces above ground, the navigable air space within a person's private property to control the proliferation of data emitting from the private residence? Concerns of licensing and manageability of drones could easily stimulate research that address data storage, rights and ownership of drone media, and legalities homeowners and drone operators may face in planned and unplanned neighborhood drone operations. When will laws, policies, or legal processes be established that can be injected in residential areas before harm reaches within the home and negatively affects the well-being of residents? Will it be when a UAS begins to track our alarm clocks, channel the start and movement of our vehicle when departing from home, intercept the audible beeps to an alarm system for replay, or even target the movement of a young child awakening or any person in some form, which could lead to abduction?

Future researchers could delve deeper to address various privacy issues between different types of drones, how they could be affected by hacking, or a research to discover routes and vulnerabilities of data discovered by drones through WIFI capabilities. The 21 October 2016 distributed denial-of-service (DDoS) attack was indicative of just how residential cyber devices could be used to cause catastrophic interruptions without the residential owners' knowledge (O'Brien, 2016). Using drones is just one of the means data could be intercepted to gain visual and physical access to a victim's property in real-time. The DHS issued a fact sheet back in April 2016 titled, "Homeland Security Starts with Hometown Security"; however, the document is really geared toward businesses. It is recommended the DHS tweak the information addressed in this fact sheet and direct attention to residential neighborhoods.

O'Brien (2016) was one of many to report on the massive 21 October DDoS attack and reporters like Perlroth (2016) noted hackers used IoT devices, e.g. wireless residential video cameras and wireless routers, in the mischievous act. Hackers ran malware that armed the IoT devices into Internet weapons and caused major disruptions to many major websites, e.g. Netflix and Twitter (Perlroth, 2016). Even on a smaller scale, it is quite possible for a perpetrator to use a drone and usurp IoT devices, disable security, and initiate a DoS attack to prevent a home monitoring security service from detecting or responding to the residence under fire or during a home invasion.

The world is finally seeing the magnitude of the Internet of Things and while there was no case identified in this writing to address a violation of drones collecting or even connecting to a resident's cyber device, it may only be with time a drone or UAS will be used to implant ransomware into private residential cyber devices; only, it is likely time will tell. This study showed there is a need to address legalities of drones and UAS' operating in residential areas where interception of data and access to cyber devices operating within those homes could possibly occur. There is also a great desire for residential cybersecurity and awareness training for information assurance disciplines that could be applied throughout residential cyber domains in residential operations and in the quest for residential privacy through cybersecurity. Finally, there is a void in residential understanding of technological developments using drones in residential package deliveries could subject one or more individuals to an invasion of privacy.

Summary

With drones and IoT, study participants perceived their privacy rights were susceptible to compromise when associated with private, individual use of drones operated in a Maryland residential area. The problem driving this qualitative phenomenological research study was based on an implication drones sold for recreational purposes at record paces were being manipulated through areas where unlawful viewing and data collection of a person's private area occur (Choi-Fitzpatrick, 2014). The purpose of this qualitative phenomenological research was to understand how private citizens perceived privacy when drones flown over their residences could access cyber devices operating within their homes. Contribution of information to the overall body of knowledge showed there is a significant need to continue this research for legal, educational, and technological results beneficial to residential users to protect their privacy and cyber domains from unwarranted and illegal monitoring, interception, or use of private data.

The research methodology consisted of a qualitative phenomenological approach allowed the gathering of information through an online SurveyMonkey questionnaire and analysis tool permitted organization, development, distribution, and management in the singular and self-evident content analysis of participant surveys. Four major thematic areas were discovered amongst 17 categories of information used in the submission of four recommendations to educate, inject policy, and enforce newfound laws that could protect private citizen’s devices and information in cyber and wireless transmissions. Lastly, IoT is real in every aspect of our daily lives and the adage of “what you don’t know won’t hurt you” goes out the window, because in the multiplicity of cyber activities, we may very well never know what activity caused a demise or transgression of inappropriate access and manipulation of residential private information.

References

Aeronautics and Space, 14 e-C.F.R. (2015) (49 U.S.C. 106(g), 40113, 44701), 11. Retrieved from https://www.gpo.gov/fdsys/pkg/CFR-2004-title14-vol1/pdf/CFR-2004-title14-vol1-chapI-subchapA.pdf

Ahn, J., Bang, Y., & Lee, D. (2011). Managing consumer privacy concerns in personalization: A strategic analysis of privacy protection. *MIS Quarterly, 35*(2). Retrieved from http://web.b.ebscohost.com/

Akkoyunlu, B. & Daghan, G. (2014). A qualitative study about performance based assessment methods used in information technologies lesson. *Educational Sciences: Theory and Practice, 14*(1). Retrieved from http://web.b.ebscohost.com/

Aluwihare-Samaranayake, D. (2012). Ethics in qualitative research: A view of the participants' and researchers' world from a critical standpoint. *International Journal of Qualitative Methods, 11*(2). Retrieved from http://web.a.ebscohost.com/

Anderson, C. (2013). *Under every Christmas tree: A drone*. Retrieved from http://web.a.ebscohost.com/

Anderson, K., DeBell, L., Duffy, J. P., Griffiths, A., Griffiths, D., Hancock, S., Reinhardt, W. J., & Shutler, J. D. (2016). A grassroots remote sensing toolkit using live coding, smartphones, kites and lightweight drones. *PLoS ONE, 11*(5). doi:10.1371/journal.pone.0151564

Anteunis, L. C., Joore, M. A., Linssen, A. M., Minten, R. K., & van Leeuwen, Y. D. (2013). Qualitative interviews on the beliefs and feelings of adults towards their ownership, but non-use of hearing aids. *International Journal of Audiology, 52*(10). doi:10.3109/14992027.2013.808382

Applebaum, M. (2012). Phenomenological psychological research as science. *Journal of Phenomenological Psychology, 43*(1), 48. doi:10.1163/156916212X632952

Aquino-Segarra, O. (2016). Drones: The need for more regulations. *Revista De Derecho Puertorriqueño, 55*(2). Retrieved from http://web.b.ebscohost.com

Arapinis, M., Bursuc, S., & Ryan, M. (2013). Privacy-supporting cloud computing by in-browser key translation. *Journal of Computer Security, 21*(6). doi:10.3233/JCS-130489

Armayor, N. C., McQueen, A., Vivar, C. G., & Whyte, D. A. (2007). Getting started with qualitative research: Developing a research proposal. *Nurse Researcher, 14*(3). Retrieved from http://web.b.ebscohost.com

Arquero, O., López-Granados, F., Peña, J. M., Serrano, N., & Torres-Sánchez, J. (2015). High-throughput 3-D monitoring of agricultural-tree plantations with unmanned aerial vehicle (UAV) technology. *PLOS ONE, 10*(6). doi:10.1371/journal.pone.0130479

Atherton, K. (2015, August 11). Drone at DEFCON hacks from the sky: Snoops that swoop. *Popular Science.* Retrieved from http://www.popsci.com/drone-defcon-hacks-sky

Barocas, S., & Nissenbaum, H. (2014, November). Computing ethics: Big data’s end run around procedural privacy protections. *Communications of the ACM, 57*(11). doi:10.1145/2668897

Barr, D. B., Bradman, A., Fenske, R. A., Whyatt, R. M., & Wolff, M. S. (2005). Lessons learned for the assessment of children’s pesticide exposure: Critical sampling and analytical issues for future studies. *Environmental Health Perspectives, 113*(10). doi:10.1289/ehp.7674

Barry, T. (2013). Drones over homeland: Expansion of scope and lag in governance. *The Brown Journal of World Affairs, 19*(2). Retrieved from http://search.proquest.com/docview/1649691379?accountid=44888

Bewley-Taylor, D. (2005). US concept wars, civil liberties and the technologies of fortification. *Crime, Law and Social Change, 43*(1). doi:10.1007/s10611-005-4054-z

Billi, C. (2015, June 6). Drone ban and other new laws land in Florida. WTSP, 10 News, Tampa, Florida. Retrieved from http://www.wtsp.com/story/news/local/2015/06/30/new-drone-laws-flying-into-florida/29546665/

Blalock, E. N., & Gilchrest, B. A. (2013, July). As I said before. *Journal of Investigative Dermatology, 133*(7). doi:10.1038/jid.2012.342

Brandeis, L. D. & Warren, S. V. (1890). The right to privacy. *Harvard Law Review, 4*(5). Retrieved from ebscohost.com

Brouwer, R. L., de Schipper, M. A., Rynne, P. F., Graham, F. J., Reniers, A. M., & MacMahan, J. H. (2015). Surfzone monitoring using rotary wing unmanned aerial vehicles. *Journal of Atmospheric & Oceanic Technology, 32*(4). doi:10.1175/JTECH-D-14-00122.1

Cai, C., Cai, G., Xu, J., & Zou, Y. (2016). Robust H∞ control for miniature unmanned aerial vehicles at hover by the finite frequency strategy. *IET (The Institution of Engineering and Technology) Control Theory & Applications, 1*0(2). doi:10.1049/iet-cta.2015.0641

Caine, K., Fisk, A., & Rogers, W. (2005). Privacy perceptions of an aware home with visual sensing devices. *Proceedings of the Human Factors and Ergonomics Society, USA,* (49th annual meeting). Retrieved from http://pro.sagepub.com

Calo, R., Schmiedeskamp, P., Simon, M., Whittington, J., Woo, J., & Young, M. (2015). Push, pull, and spill: A transdisciplinary case study in municipal open government. *Berkeley Technology Law Journal, 30*(3). doi:10.15779/Z38PZ61

Capello, E., Guglieri, G., Quagliotti, F., & Scola, A. (2012). Mini quadrotor UAV: Design and experiment. *Journal of Aerospace Engineering, 25*(4). doi:10.1061/(ASCE)AS.1943-5525.0000171

Cassell, C., & Symon, G. (2011). Assessing 'good' qualitative research in the work psychology field: A narrative analysis. *Journal of Occupational & Organizational Psychology, 84*(4). doi:10.1111/j.2044-8325.2011.02009.x

Choi-Fitzpatrick, A. (2014). Drones for good: Technological innovations, social movements, and the state. *Journal of International Affairs, 68*(1). Retrieved from http://web.b.ebscohost.com/

Chrousos, G. P., Gravanis, A., Kalantaridou, S. N., & Margioris, A. N. (2012). The 'self-plagiarism' oxymoron: Can one steal from oneself? *European Journal of Clinical Investigation, 42*(3). doi:10.1111/j.1365-2362.2012.02645.x

Chur-Hansen, A., Crawford, G. B., & Ng, F. (2014). How do palliative medicine specialists conceptualize depression? Findings from a qualitative in-depth interview study. *Journal of Palliative Medicine, 17*(3). doi:10.1089/jpm.2013.0378

Clark, V., & Creswell, J. (2011). *Designing and conducting mixed methods research* (2nd ed.). Thousand Oaks, CA: Sage.

Cleary, M., Hayter, M., & Horsfall, J. (2014, April). Qualitative research: Quality results? *Journal of Advanced Nursing (JAN)*. doi:10.1111/jan.12172

Cloud. (n.d.). *In Merriam-Webster's online dictionary* (11th ed.). Retrieved from http://www.merriam-webster.com/dictionary/cloud

Colyar, J. & Holley, K. (2012). Under construction: How narrative elements shape qualitative research. *Theory Into Practice, 51*(2). doi:10.1080/00405841.2012.662866

Committee on National Security Systems (CNSS). (2015, April). *National information assurance glossary* (CNSS Instruction 4009). Retrieved from http://www.fas.org

Cone, J. D., & Foster, S. L. (2006). *Dissertations and Theses from Start to Finish* (2nd ed.). Washington, D.C.: American Psychological Association.

Congressional Research Service (CRS). (2015). *Domestic drones and privacy: A primer* (CRS R43965). Retrieved from https://www.crs.gov

Conrad, F., Lind, L., Reichert, H., & Schober, M. (2013). Why do survey respondents disclose more when computers ask the questions? *Public Opinion Quarterly, 77*(4). doi:10.1093/poq/nft038

Costante, E., Hartog, J., & Petković, M. (2015). Understanding perceived trust to reduce egret. *Computational Intelligence, 31*(2). doi:10.1111/coin.12025

Creswell, J. W. (2012). *Educational research*: *Planning, conducting, and evaluating quantitative and qualitative research* (4th ed.), 306. Upper Saddle River, NJ: Pearson.

Creswell, J. W., & Plano Clark, V. L. (2011). *Designing and conducting mixed methods research* (2nd ed.). Thousand Oaks, CA: Sage.

Cross, E. S., Hamilton, A. F., & Ramsey, R. (2012). Predicting others' actions via grasp and gaze: Evidence for distinct brain networks. *Psychological Research, 76*(4). doi:10.1007/s00426-011-0393-9

Crowsey, R. C., Kar, B., & Zale, J. J. (2013). The myth of location privacy in the United States: Surveyed attitude versus current practices. *Professional Geographer*, *65*(1). doi:10.1080/00330124.2012.658725

Demchak, C. C., & Fenstermacher, K. D. (2009). Institutionalizing behavior-based privacy. *Administration and Society, 47*(7). doi:0.1177/0095399709344047

Denning, P. J., & Frailey, D. J. (2011). The Profession of IT: Who are we- Now? *Communications of the ACM, 54*(6). doi:10.1145/1953122.1953133

Denscombe, M. (2009). Item non-response rates: A comparison of online and paper questionnaires. *International Journal of Social Research Methodology, 12*(4). doi:10.1080/13645570802054706

DHS. (2016, April). *Homeland security starts with hometown security*. Factsheet. Retrieved from https://www.dhs.gov

DHS. (n.d.). *Stop. Think. Connect. Cybersecurity 101*. Retrieved from https://www.dhs.gov/sites/default/files/publications/cybersecurity-101_4.pdf

Dilles, T., Diltour, N., Havens, D. S., Peremans, L., Van Bogaert, P., Van heusden, D., & Van Rompaey, B. (2016). Staff nurses' perceptions and experiences about structural empowerment: A qualitative phenomenological study. *Plos ONE, 11*(4). doi:10.1371/journal.pone.0152654

Dolan, A. M., & Thompson, R. M., II. (2013). Integration of drones into domestic airspace: Selected legal issues [January 30, 2013]. Retrieved from https://www.hsdl.org/?view&did=730503

Drone. (n.d.). *In Merriam-Webster's online dictionary* (11th ed.). Retrieved from http://www.merriam-webster.com/dictionary/drone

Eckartsberg, R. (2010). On the geography of human experience. *Humanistic Psychologist, 38*(3). doi:10.1080/08873261003635997

Englander, M. (2012). The interview: Data collection in descriptive phenomenological human scientific research. *Journal of Phenomenological Psychology, 43*(1). doi:10.1163/156916212X632943

Erkip, F., & Mugan, G. (2010). Increasing the effectiveness of time-use survey with qualitative methods: The analysis of time-space interaction. *Innovation - The European Journal of Social Sciences, 23*(3). doi:10.1080/13511610.2010.543530

FAA Modernization and Reform Act of 2012, Pub. L. No.112–95, 331, 126 Stat. (2012).

Fawcett, J. (2011, October). Editor's choice. *Journal of Advanced Nursing (JAN).* doi:10.1111/j.1365-2648.2011.05818.x.

FBI. (2015, September). Alert number I-091015-PSA. Public Service Announcement: Federal Bureau of Investigation. Internet of things poses opportunities for cyber crime. Retrieved from https://www.ic3.gov/media/2015/150910.aspx

FBI. (2016, October). National cyber security awareness month: Cyber security is everyone’s responsibility. Retrieved from https://www.fbi.gov

Finfgeld-Connett, D., & Johnson, E. D. (2012). Literature search strategies for conducting knowledge-building and theory-generating qualitative systematic reviews. *Journal of Advanced Nursing, 69*(1). doi:10.1111/j.1365-2648.2012.06037.x

Freedom from Unwarranted Surveillance Act (FUSA), 3 Fla. Stat. § 934.50 Title XLVII. (2015).

Garton, S., Robertson, S., White, G., & White, S. (2012). Disorderly houses: Residences, privacy, and the surveillance of sexuality in 1920s Harlem. *Journal of the History of Sexuality, 21*(3). doi:10.7560/JHS21303

Giorgi, A. (2012). The descriptive phenomenological psychological method. *Journal of Phenomenological Psychology, 43*(1). doi:10.1163/156916212X63293

Goldman, J., Kitto, S., Peller, J., & Reeves, S. (2013). Ethnography in qualitative educational research: AMEE Guide No. 80. *Medical Teacher, 35*(8). doi:10.3109/0142159X.2013.804977

Green, H. E. (2014). Use of theoretical and conceptual frameworks in qualitative research. *Nurse Researcher, 21*(6). Retrieved from http://web.b.ebscohost.com/

Haahr, A., Hall, E. O., & Norlyk, A. (2014). Ethical challenges embedded in qualitative research interviews with close relatives. *Nursing Ethics*, *21*(1). doi:10.1177/0969733013486370

Haegele, J. A., & Hodge, S. R. (2015). Quantitative methodology: A guide for emerging physical education and adapted physical education researchers. *Physical Educator, 72*. Retrieved from http://web.b.ebscohost.com/

Hamari, J., Karvonen, K., Lampinen, A., Oulasvirta, A., & Suomalainen, T. (2014). Transparency of intentions decreases privacy concerns in ubiquitous surveillance. *Cyberpsychology, Behavior & Social Networking*, *17*(10). doi:10.1089/cyber.2013.0585

Harding, B., Hume, S., Lapum, J. L., Liu, L., Nguyen, M., Siyuan, W., & Yau, T. M. (2015). Pictorial narrative mapping as a qualitative analytic technique. *International Journal of Qualitative Methods, 14*(5). doi:10.1177/1609406915621408

Harrington, A. (2015). Who controls the drones? *Engineering & Technology, 10*(2). Retrieved from http://web.b.ebscohost.com/

Harrington, A., King, L., & McCloud, C. (2013). A qualitative study of regional anaesthesia for vitreo-retinal surgery. *Journal of Advanced Nursing, 70*(5). doi:10.1111/jan.12263

Harris, K. (2013). Disallowing recommendations for practice and policy: A proposal that is both too much and too little. *Educational Psychology Review, 25*(3). doi:10.1007/s10648-013-9235-1

Hutchins, A., & McNeill, J. (2015, Summer). The anatomy of information: Bio-data and wearable technology under examination. *Science and Technology*. Phi Kappa Phi Forum, *95*(2). Retrieved from http://web.b.ebscohost.com

IoT. (n.d.). Internet of things tip card. Retrieved from https://www.dhs.gov/sites/default/files/publications/Internet%20of%20Things%20Tip%20Card_3.pdf

Jacobstein, N. (2013). Drones: A 360 degree view. *World Policy Journal, 30*(3). doi:10.1177/0740277513506376

Jones, J., & Mealer, M. (2014). Methodological and ethical issues related to qualitative telephone interviews on sensitive topics. *Nurse Researcher*, *21*(4). Retrieved from http://web.b.ebscohost.com/

Jones, M. V. (2014). Drones the sky's the limit - or is it? *Technology and Engineering Teacher, 74*(1). Retrieved from ebscohost.com

Kim, J., Kwon, J., & Seo, J. (2014, September). Robotic explorers. *Electronics Letters, 50*(20). (Electronics Letters is the property of Institution of Engineering & Technology). doi:10.1049/el.2014.3309

Kimantas, J. (2014). Up close, it's personal. *Alternatives Journal (A\J) - Canada's Environmental Voice, 40*(3). Retrieved from http://web.a.ebscohost.com/

Knapik, M. (2006). The qualitative research interview: Participants' responsive participation in knowledge making. *International Journal of Qualitative Methods, 5*(3). Retrieved from http://web.b.ebscohost.com/

Licqurish, S., & Seibold, C. (2011). Applying a contemporary grounded theory methodology. *Nurse Researcher, 18*(4). Retrieved from http://web.b.ebscohost.com/

Mack, T. C. (2014). Privacy and the surveillance explosion. *The Futurist, 48*(1). Retrieved from http://web.b.ebscohost.com/

Magilvy, J. K., & Thomas, E. (2011). Qualitative rigor or research validity in qualitative research. *Journal For Specialists In Pediatric Nursing, 16*(2). doi:10.1111/j.1744-6155.2011.00283.x

Marris, E. (2013). Drones in science: Fly, and bring me data. *Nature*, *498*. doi:10.1038/498156a

Maryland (State). Legislature. Assembly. *Criminal procedure – Government drone use - Limitations*. 351. 2016 Reg. Sess. Withdrawn. (February 29, 2016). *Maryland General Assembly*. House. Web. 10 Jul. 2016.

Maryland (State). Legislature. Assembly. *Drones – Unauthorized surveillance*. 785. 2014 Reg. Sess. (March 13, 2014). *Maryland General Assembly*. House. Web. 10 Jul. 2016.

McBride, D., & Stough, R. (2014). Big data and U. S. public policy. *Review of Policy Research, 31*(4). doi:10.1111/ropr.12083

Melling, B. & Slife, B. (2012). Method decisions: Quantitative and qualitative inquiry in the study of religious phenomena. *Pastoral Psychology, 61*(5/6). doi:10.1007/s11089-011-0366-3

Metcalfe, A. & Newington, L. (2014). Factors influencing recruitment to research: Qualitative study of the experiences and perceptions of research teams. *BMC* [BioMed Central] *Medical Research Methodology, 14*(1). doi:10.1186/1471-2288-14-10

Miami-Dade Police Department. (2014). 2014 Florida Law Enforcement Handbook: Miami-*Dade County Edition* (Pub. 23154). Retrieved from http://www.leg.state.fl.us

Miller, J. (2015). New age tracking technologies in the post-United States v. Jones environment: The need for model legislation. *Creighton Law Review, 48*(3). Retrieved from http://web.b.ebscohost.com/

Mills, M. (2015). Know your drone. *Planning, 81*(5). Retrieved from http://web.b.ebscohost.com/

Molko, R. (2013). The drones are coming! Will the Fourth Amendment stop their threat to our privacy? *Brooklyn Law Review, 78*(4). Retrieved from http://brooklynworks.brooklaw.edu/blr/vol78/iss4/3

Mort, M., Shelton, C. L., & Smith, A. F. (2014). Opening up the black box: An introduction to qualitative research methods in anaesthesia. *Anaesthesia, 69*(3). doi:10.1111/anae.12517

Nagy, B. (2014). Why they can watch you: Assessing the constitutionality of warrantless unmanned aerial surveillance by law enforcement. *Berkeley Technology Law Journal, 29*(1), 148. Retrieved from http://web.b.ebscohost.com/

National Institute of Standards and Technology (NIST). (2015). *NIST big data interoperability framework: Volume 1, definitions* (NIST SP 1500-1). Retrieved from http://www.nist.gov/manuscript-publication-search.cfm?pub_id=918927

Neil, B. A., & Neil II, B. A. (2013). Police drones: A legal studies case study. *Journal of Business Case Studies* [online], *9*(5), 354. Retrieved from http://search.proquest.com/docview/1433048998?accountid=44888

NIST. (2013). *Glossary of key information security terms* (NISTIR 7298), *2*, retrieved from http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

NIST. (2016). *Networks of 'things'* (NIST SP 800-183). Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf

NIST. (2015). *The NIST definition of cloud computing* (NIST SP 800-145). Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

O'Brien, S. (2016, October 21). Widespread cyberattack takes down sites worldwide. *CNN Money*. Retrieved from http://www.money.cnn.com

Pau, G., Tesoriere, G., & Tirrito, S. (2015). A Fuzzy Controller to Reduce Power Consumption in a Quadrotor Helicopter for Environmental Monitoring. *AIP Conference Proceedings*, *1648*(1). doi:10.1063/1.4912989

Paust, J. J. (2015). Can you hear me now? Private communication, national security, and the human rights disconnect. *Chicago Journal of International Law*, *15*(2). Retrieved from http://search.proquest.com/docview/1651730653?accountid=44888

Peppet, S. R. (2014). Regulating the Internet of things: First steps toward managing discrimination, privacy, security, and consent. *Texas Law Review, 93*(1), 13. Retrieved from http://web.b.ebscohost.com/

Perlroth, N. (2016, October 21). Hackers used new weapons to disrupt major websites across U.S. *The New York Times*. Retrieved from http://www.nytimes.com

Pomeroy, C. J. (2015). All your air right are belong to us. *Journal of International Human Rights, 13*(3). Retrieved from http://web.a.ebscohost.com/

Price-Williams, A. (2015). *Resolution supporting SB 510 or similar legislation that would provide criminal penalties for convicted sexual predators who use or operate a drone to view or record an image of a minor under certain circumstances* [Memorandum]. Miami, FL: Miami-Dade County Attorney.

Protection of Human Subjects, 45 C.F.R. pt. 46 (2009).

Ransomware. (n.d.). *In Department of Homeland Security keywords*. Retrieved from https://www.dhs.gov/keywords/malware

Rausch, R. L. (2011). Refraining Roe: Property over privacy. *Berkeley Journal of Gender, Law & Justice*, *27*(1). Retrieved from http://web.a.ebscohost.com/

Reynolds, D. L. (1978). O.S.H.A. and the Fourth Amendment. *Human Resource Management (Pre-1986), 17*(3). Retrieved from http://search.proquest.com/docview/223824580?accountid=44888

Salkind, N. (2012). *Exploring research*. Upper Saddle River, NJ: Pearson Education Inc., *8*(10).

Sanders, R. J. (2015). "I'll be watching you": The Florida voyeurism offense. *Florida Bar Journal, 89*(2). Retrieved from http://web.a.ebscohost.com/

S. C. Code of Laws 16-17-470. Eavesdropping, peeping, voyeurism.

Serial No. J-113-10: *The future of drones in America: Law enforcement and privacy considerations, United States Senate*, 113th Cong (2013) (testimony of Amie Stepanovich).

Shannon-Baker, P. (2015). "But I wanted to appear happy": How using arts-informed and mixed methods approaches complicate qualitatively driven research on culture shock. *International Journal of Qualitative Methods, 14*(2). Retrieved from http://web.b.ebscohost.com

Snelgrove, S. R. (2014). Conducting qualitative longitudinal research using interpretative phenomenological analysis. *Nurse Researcher, 22*(1). Retrieved from http://web.b.ebscohost.com

Snelson, C. L. (2016). Qualitative and mixed methods social media research: A review of the literature. *International Journal of Qualitative Methods*, 1-15. doi:10.1177/1609406915624574

Stahl, R. (2013). What the drone saw: The cultural optics of the unmanned war. *Australian Journal of International Affairs, 67*(5). doi:10.1080/10357718.2013.817526

Stephens, G. (2013). Crime in the year 2030. *The Futurist, 47*(1). Retrieved from http://search.proquest.com/docview/1267121024?accountid=44888

Sterio, M. (2012). The United States' use of drones in the war on terror: The (il)legality of targeted killings under international law. *Case Western Reserve Journal of International Law, 45*. Retrieved from http://web.b.ebscohost.com

Stevens, L. & Wells, G. (2016, September 23). UPS uses drones to deliver package to Boston-area Island. *The Wall Street Journal*. Business, Logistics Report. Retrieved from http://www.wsj.com/articles/ups-uses-drone-to-deliver-package-to-boston-area-island-1474662123

Subbaraman, N. (2013, May 17). Should FBI manhunts use drones? US lawmakers debate. *NBC News*. Retrieved from http://www.nbcnews.com/

Takahashi, T. (2012). Drones and privacy. *The Columbia Science and Technology Law Review. 14* (Rev. 73). Retrieved from http://www.stlr.org/cite.cgi?volume=14&article=2

Terwilliger, B. A. (2013). How can higher education best support UAS growth in America? *Collegiate Aviation Review*, *31*(2). Retrieved from http://web.b.ebscohost.com

Thompson, R. M., II. (2015). Domestic drones and privacy: A primer [March 30, 2015]. Retrieved from https://www.hsdl.org/

United States. Executive Office of the President. (2014). Big data: Seizing opportunities, preserving values. Retrieved from https://www.hsdl.org/?view&did=752636

U.S. Const. Amend. IV (1791).

Vilalta, C. J. (2012). Fear of crime and home security systems. *Police Practice & Research*, *13*(1). doi:10.1080/15614263.2011.607651

Villasenor, J. (2013). Observations from above: Unmanned aircraft systems and privacy. *Harvard Journal of Law & Public Policy, 36*(2). Retrieved from http://web.b.ebscohost.com

Volokh, E. (2014). Tort law vs. privacy. *Columbia Law Review*, *114*. Retrieved from http://search.proquest.com/docview/1564109491?accountid=44888

Wagstaff, C., & Williams, B. (2014). Specific design features of an interpretative phenomenological analysis study. *Nurse Researcher*, *21*(3). Retrieved from http://web.b.ebscohost.com/

Wahlstrom, N. (2008). After decentralization: Delimitations and possibilities within new fields. *Journal of Curriculum Studies, 40*(6). doi:10.1080/00220270801975379

Wolper, M. (2012). Manifest disregard. *Florida Bar Journal, 86*(8). Retrieved from http://web.b.ebscohost.com

Appendix A: Literature Search

Key Word Search	Peer Reviewed Works Reviewed	Germinal Works Reviewed	Books Reviewed	Studies Reviewed	Totals
Cybersecurity	18				18
Drones	39	1			40
Privacy Policies	39				39
Privacy Rights	15				15
Security Challenges	11				11
Unmanned Aerial System	7				7
Unmanned Aerial Vehicle	11				11
Research Methodologies					
Qualitative Analysis	48	1	4		53
Quantitative Analysis	5				5
Mixed Methods	9		3		12
Total Documents Reviewed	**202**	**2**	**7**	**0**	**211**

Table 45: Literature Search Summary

Appendix B: Informed Consent Letter

Dear ___________________________:

My name is Sandra A. Wright and I am a doctoral candidate at Capitol Technology University located in Laurel, Maryland. This letter is in two parts: Part A is to provide details to you of this request; and Part B is the Informed Consent Form for you to complete and return to me before the interview.

PART A – Study Information

You have been identified as a viable participant in a study on drones, titled, "Drones: Discovering Perceptions of an Invasion of Privacy in Residential Areas". Participation in this study is purely voluntary and requires no commitment from you of any sort. If you decide to participate in this study, please know that you may withdraw at any time.

The purpose of this research is to understand how private citizens perceive privacy when drones flown over their residences could access cyber devices operating within their homes. A brief questionnaire was developed for use in the data collection during a 15 to 30-minute interview of each participant. Your interview will be recorded and the recorded data will be transcribed later for use in the final study results and maintained within legal bounds.

Obtaining details of your experience will help me to understand more about the subject and possibly help improve residential knowledge of drones, security of cyber devices, and your privacy rights. Your name is only for identification purposes, clarification, and follow-up if needed; only researchers associated with this study will have access to these details. There are no known risks connected with the study, but I will be happy to provide the results of this study to you once the research is complete.

Sandra A. Wright   _______________
Capitol Technology University   Date
Doctoral Candidate

PART B – Informed Consent Form

I acknowledge an understanding of the above information and that my participation in the study on "Drones: Discovering Perceptions of an Invasion of Privacy in Residential Areas" is completely voluntary. I understand my interview will be recorded, used in the study results, and personal information handled as confidential. I am also acknowledging receipt of a copy of this consent form for my records.

Printed Name: ________________________ ______________ _______________________
First   Middle   Last

____   _______________________
Signature   Date

Appendix C: Survey Questions

Survey on Drones: Discovering Perceptions of an Invasion of Privacy in Residential Areas

***1 Would you like to participate in this survey?**

○ Yes

○ No

50%

Next

Survey on Drones: Discovering Perceptions of an Invasion of Privacy in Residential Areas

*2 What is your age?

○ 18 to 24
○ 25 to 34
○ 35 to 44
○ 45 to 54
○ 55 to 64
○ 65 to 74
○ 75 or older

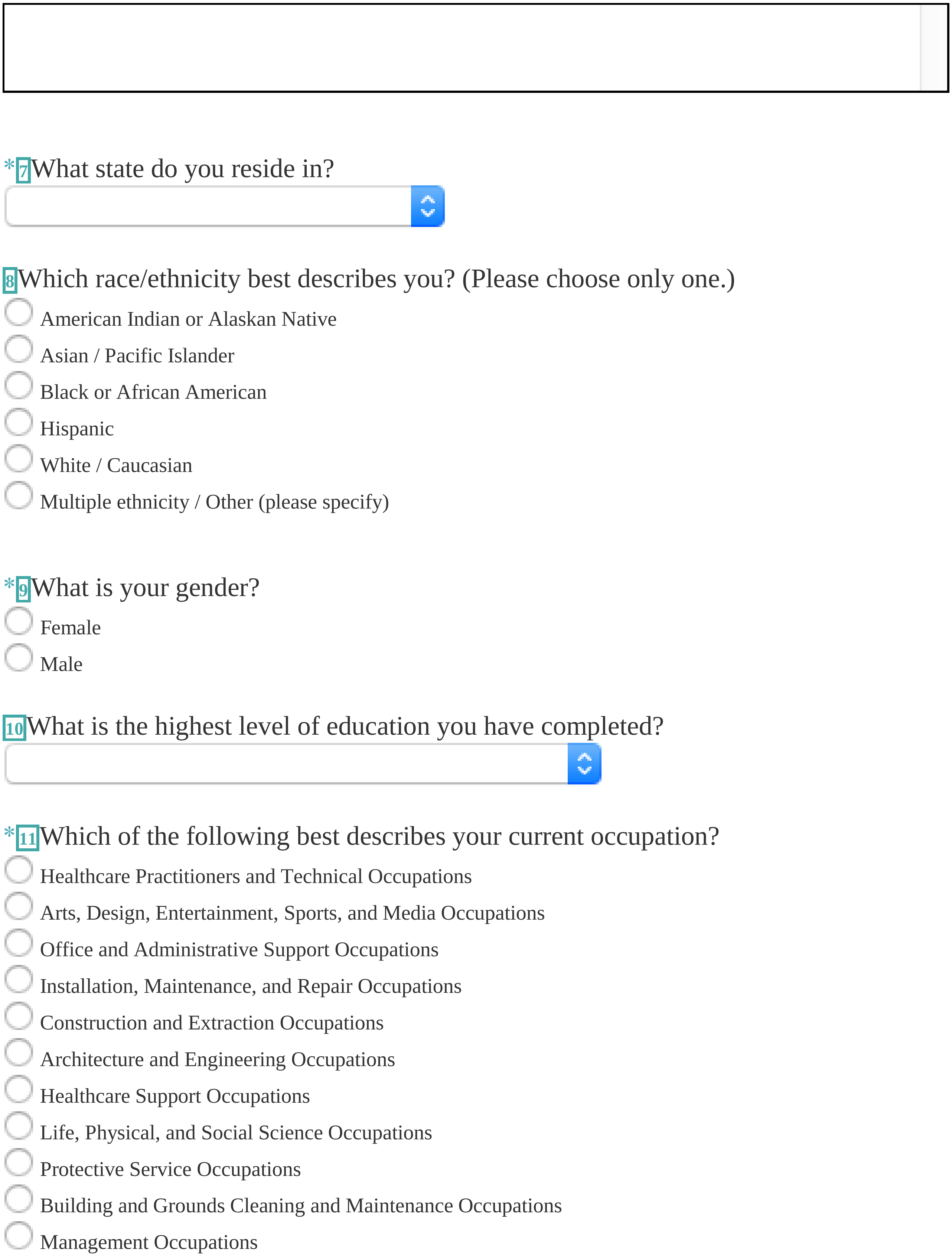
*3 Do you give your permission to have a tape-recorded interview of this survey? An interview will allow the interviewer to go through the survey with you and provide clarification on any unanswered questions in the survey.

○ Yes
○ No

*4 What is your first name?

5 What is your last name?

*6 In what city do you live?



*7 What state do you reside in?

8 Which race/ethnicity best describes you? (Please choose only one.)

○ American Indian or Alaskan Native
○ Asian / Pacific Islander
○ Black or African American
○ Hispanic
○ White / Caucasian
○ Multiple ethnicity / Other (please specify)

*9 What is your gender?

○ Female
○ Male

10 What is the highest level of education you have completed?

*11 Which of the following best describes your current occupation?

○ Healthcare Practitioners and Technical Occupations
○ Arts, Design, Entertainment, Sports, and Media Occupations
○ Office and Administrative Support Occupations
○ Installation, Maintenance, and Repair Occupations
○ Construction and Extraction Occupations
○ Architecture and Engineering Occupations
○ Healthcare Support Occupations
○ Life, Physical, and Social Science Occupations
○ Protective Service Occupations
○ Building and Grounds Cleaning and Maintenance Occupations
○ Management Occupations

○ Computer and Mathematical Occupations
○ Sales and Related Occupations
○ Education, Training, and Library Occupations
○ Legal Occupations
○ Personal Care and Service Occupations
○ Business and Financial Operations Occupations
○ Food Preparation and Serving Related Occupations
○ Farming, Fishing, and Forestry Occupations
○ Community and Social Service Occupations
○ Production Occupations
○ Transportation and Materials Moving Occupations
○ Other (please specify)

12 How much total combined money did all members of your HOUSEHOLD earn last year?

○ $0 to $9,999
○ $10,000 to $24,999
○ $25,000 to $49,999
○ $50,000 to $74,999
○ $75,000 to $99,999
○ $100,000 to $124,999
○ $125,000 to $149,999
○ $150,000 to $174,999
○ $175,000 to $199,999
○ $200,000 and up
○ Prefer not to answer

13 What do you know about drones?

14 What is your experience with drones flown in any residential area?

15 What day of the week and time of day have you experienced a drone flying in your neighborhood?

	Morning (5:00 a.m. to noon)	Afternoon (noon to 6:00 p.m.)	Evening/Night (after 6:00 p.m.)
Sunday	□ Sunday Morning (5:00 a.m. to noon)	□ Sunday Afternoon (noon to 6:00 p.m.)	□ Sunday Evening/Night (after 6:00 p.m.)
Monday	□ Monday Morning (5:00 a.m. to noon)	□ Monday Afternoon (noon to 6:00 p.m.)	□ Monday Evening/Night (after 6:00 p.m.)
Tuesday	□ Tuesday Morning (5:00 a.m. to noon)	□ Tuesday Afternoon (noon to 6:00 p.m.)	□ Tuesday Evening/Night (after 6:00 p.m.)
Wednesday	□ Wednesday Morning (5:00 a.m. to noon)	□ Wednesday Afternoon (noon to 6:00 p.m.)	□ Wednesday Evening/Night (after 6:00 p.m.)
Thursday	□ Thursday Morning (5:00 a.m. to noon)	□ Thursday Afternoon (noon to 6:00 p.m.)	□ Thursday Evening/Night (after 6:00 p.m.)
Friday	□ Friday Morning (5:00 a.m. to noon)	□ Friday Afternoon (noon to 6:00 p.m.)	□ Friday Evening/Night (after 6:00 p.m.)
Saturday	□ Saturday Morning (5:00 a.m. to noon)	□ Saturday Afternoon (noon to 6:00 p.m.)	□ Saturday Evening/Night (after 6:00 p.m.)

16 Which of the following devices do you most often use to connect to the Internet?

○ Enterprise digital assistant (EDA)
○ Laptop computer
○ Personal digital assistant (PDA)
○ Computer tablet
○ Desktop computer
○ Smart phone
○ Other (please specify)

17 What do you think about drones entering your private spaces, accessing your cyber/wireless devices, creating data about you, and placing that data in a cloud?

18 Describe your cybersecurity practices for new Internet or web-enabled cyber/wireless devices entering your residential space (e.g. When a visitor arrives with an internet-ready/WI-FI crockpot for a barbecue or cookout).

19 What precautions do you take to securely perform sensitive activities (e.g. banking) when using cyber/wireless devices?

20 Who would you call or notify if you suspect unauthorized activity (e.g. unauthorized surveillance or possible electronic ransom) on any of your cyber/wireless devices in your home? Why would you select that person?

21 What cyber/wireless device and what actions can your provider take to remotely control their device without your permission or knowledge? (For example, your cable provider may send periodic updates to their WiFi-enabled set top box to provide a new capability or correct a vulnerability.)

*22How concerned are you if a drone has the capability to pickup and record wireless signals from within your residential domain?

On a scale from 1 (not) to 5 (extremely), please rate how concerned you are with each device. By concerned, it means the more concerned you are about a device, the higher you would rate it. The less concerned you are about a device, the lower you would rate it.

	Not applicable	Not concerned	Slightly concerned with no protection.	Moderately concerned with some protection.	Extremely concerned, but adequately protected.	Extremely concerned; do not know what to do, no protection, or no solution.
Computer (e.g. laptop, PDA, etc.) connected via wireless network	○ Computer (e.g. laptop, PDA, etc.) connected via wireless network Not applicable	○ Computer (e.g. laptop, PDA, etc.) connected via wireless network Not concerned	○ Computer (e.g. laptop, PDA, etc.) connected via wireless network Slightly concerned with no protection.	○ Computer (e.g. laptop, PDA, etc.) connected via wireless network Moderately concerned with some protection.	○ Computer (e.g. laptop, PDA, etc.) connected via wireless network Extremely concerned, but adequately protected.	○ Computer (e.g. laptop, PDA, etc.) connected via wireless network Extremely concerned; do not know what to do, no protection, or no solution.
Other (please specify)						
Mobile phone	○ Mobile phone Not applicable	○ Mobile phone Not concerned	○ Mobile phone Slightly concerned with no protection.	○ Mobile phone Moderately concerned with some protection.	○ Mobile phone Extremely concerned, but adequately protected.	○ Mobile phone Extremely concerned; do not know what to do, no protection, or no solution.
Other (please specify)						
Wireless home phone	○ Wireless home phone Not applicable	○ Wireless home phone Not concerned	○ Wireless home phone Slightly concerned with no protection.	○ Wireless home phone Moderately concerned with some protection.	○ Wireless home phone Extremely concerned, but adequately protected.	○ Wireless home phone Extremely concerned; do not know what to do, no protection, or no solution.

	Not applicable	Not concerned	Slightly concerned with no protection.	Moderately concerned with some protection.	Extremely concerned, but adequately protected.	Extremely concerned; do not know what to do, no protection, or no solution.
Other (please specify)						
Wireless Garage Door Opener	○ Wireless Garage Door Opener Not applicable	○ Wireless Garage Door Opener Not concerned	○ Wireless Garage Door Opener Slightly concerned with no protection.	○ Wireless Garage Door Opener Moderately concerned with some protection.	○ Wireless Garage Door Opener Extremely concerned, but adequately protected.	○ Wireless Garage Door Opener Extremely concerned; do not know what to do, no protection, or no solution.
Other (please specify)						
GPS	○ GPS Not applicable	○ GPS Not concerned	○ GPS Slightly concerned with no protection.	○ GPS Moderately concerned with some protection.	○ GPS Extremely concerned, but adequately protected.	○ GPS Extremely concerned; do not know what to do, no protection, or no solution.
Other (please specify)						
Web-enabled appliance (e.g. refrigerator, air conditioner/thermostat, microwave, television)	○ Web-enabled appliance (e.g. refrigerator, air conditioner/thermostat, microwave, television) Not applicable	○ Web-enabled appliance (e.g. refrigerator, air conditioner/thermostat, microwave, television) Not concerned	○ Web-enabled appliance (e.g. refrigerator, air conditioner/thermostat, microwave, television) Slightly concerned with no protection.	○ Web-enabled appliance (e.g. refrigerator, air conditioner/thermostat, microwave, television) Moderately concerned with some protection.	○ Web-enabled appliance (e.g. refrigerator, air conditioner/thermostat, microwave, television) Extremely concerned, but adequately protected.	○ Web-enabled appliance (e.g. refrigerator, air conditioner/thermostat, microwave, television) Extremely concerned; do not know what to do, no protection, or no solution.
Other (please specify)						

23 What legal measures do you envision can be implemented to block or jam unwanted drones from capturing wireless signals from your residence?

24 What do you think about cyber/wireless capabilities to make package deliveries to your residence using drones? (It has been recently reported that drones are being used to deliver in difficult to reach locations.)

25 What notification methods would allow you to feel wireless deliveries by drones to your home are acceptable (e.g. phone calls or text messages made with at least a day’s notice)?

26 What are your thoughts about drone deliveries to your residence and giving up on your privacy to have such a wireless delivery made?

27 What local cybersecurity/wireless policies are you aware of that regulate the flying of drones in private areas, such as around your home?

28 What state cybersecurity/wireless policies are you aware of that regulate the flying of drones in private areas, such as around your home?

29 What federal cybersecurity/wireless policies are you aware of that regulate the flying of drones in private areas, such as around your home?

30 What other kind of wireless policy can be implemented to ensure web-enabled cyber devices are not intruded when there is a drone flying around your home?

31 What do you know about law enforcement’s handling of drones flown in residential areas?

32 Using a scale of 1-5, 5 being the most invasive, how would you rate drone operations in residential areas and why? By invasive, it means how threatened you think you feel by a drone flying over or near your home with the possibility of receiving wireless signals from your home cyber devices.

33 How could a no-drone-zone policy for drones be applied to residential areas? (FAA created a No-drone-policy around airports and hobbyists can fly their marked and registered, under 55 lb. drone no higher than 400 feet, but must contact airport officials if within (5) miles of an airport.)

34 What would you consider to be a reasonable fine to impose on operators when their drone attempts to connect to residential cyber/wireless devices?

*35 How does your homeowner's association address drones flown in your neighborhood?

□ Not applicable; no HOA.
□ HOA does not address drones.
□ Other (please specify)

36 How could a homeowner's association address flying drones to connect to residential cyber devices within your neighborhood?

37 What kind of cybersecurity training do you feel is needed for residences to become more knowledgeable of wireless connectivity capabilities with drones flying in residential neighborhoods?

38 What would you expect from the results of this study?

*39 How would you like to be contacted once the survey is complete and available for release?

○ No follow-up desired.

○ Please use the same email method.

○ Other (please specify, e.g. call (800) 555-1212))

100%

Prev Done

Appendix D: Major Themes and Categories

Theme #	Theme Name	Category #	Category Title	Question #	Participant Remarks
T1	Cybersecurity Practices	C01	Cybersecurity	23	P6, P8, P11, P12, and P13 felt they could offer any idea on blocking or jamming of undesirable drones from capturing wireless signals when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.
T1		C01	Cybersecurity	23	P1 considered a system shutdown to appropriately block the activity when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.
T1		C01	Cybersecurity	23	P2 and P14 shared a direct technological solution by jamming when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.
T1		C01	Cybersecurity	23	P3 indicated collection wireless signals from residential areas couldn’t be stopped when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.
T1		C01	Cybersecurity	23	P4 offered an encryption solution to ward off the unwanted capture of wireless signals when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.
T1		C01	Cybersecurity	23	P8 noted the handling was dependent on service provider-defined terms on their policy to address unwanted capture of wireless signals when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.

Theme #	Theme Name	Category #	Category Title	Question #	Participant Remarks
T1		C03	Cybersecurity practices	18	P2 and P11 indicated they have not had visitors with devices needing connection when asked to describe their cybersecurity practices for new Internet or web-enabled cyber/wireless devices entering their residential space.
T1		C03	Cybersecurity practices	18	P1 desired to keep these devices of his controlled domain when asked to describe their cybersecurity practices for new Internet or web-enabled cyber/wireless devices entering their residential space.
T1		C03	Cybersecurity practices	18	P4 through P10, and P12 through P14 practiced cybersecurity of guest connections through pre-shared keys and passwords when asked to describe their cybersecurity practices for new Internet or web-enabled cyber/wireless devices entering their residential space.
T1		C03	Cybersecurity practices	18	P3 segmented networks in trusted domains according to trusted and untrusted users; this permitted an additional layer of network protection for trusted users and cyber devices when asked to describe their cybersecurity practices for new Internet or web-enabled cyber/wireless devices entering their residential space.
T1		C03	Cybersecurity practices	19	P2 and P6 did not use cyber/wireless devices to perform sensitive activities; such as banking when asked what precautions they took to securely perform sensitive activities (e.g. banking) when they used cyber/wireless device.
T1		C03	Cybersecurity practices	19	P1, P3, P4, P5, and P7 through P13 took several precautions to ensure secure transactions over cyber/wireless devices, most commonly was the use of secure encrypted connections to trusted sites when asked what precautions they took to securely perform sensitive activities (e.g. banking) when they used cyber/wireless device.
T1		C03	Cybersecurity practices	37	P6, P8, and P13 were unsure of training deficiencies in cybersecurity in their neighborhood when asked what kind of cybersecurity training they felt was needed for residences to

Theme #	Theme Name	Category #	Category Title	Question #	Participant Remarks
					become more knowledgeable of wireless connectivity capabilities with drones flying in residential neighborhoods.
T1		C03	Cybersecurity practices	37	P1 through P5, P7, P9 through P12, and P14 desired some form of announcements, notices, education and awareness, informative meetings, and training were needed for residences to become more knowledgeable of wireless connectivity capabilities with drones flying in residential neighborhoods.
T1		C03	Cybersecurity Practices	38	P7, P9, P10, and P14 indicated the result of this study should produce more education on security risks with drones and capabilities that could access personal wireless and cyber devices, and about risks and mitigations in cybersecurity when asked what they you expected from the results of this study.
T1		C17	Technological implementations	33	P3 felt jammers could be applied in a no-drone-zone policy for drones in residential areas, but also felt defensive mechanisms could really be the best defense when asked how a no-drone-zone policy for drones could be applied to residential areas.
T1		C17	Technological implementations	33	P10 felt a technological solution that integrated residential homes into the drone application could be used to distinguish the homes as a no-drone-zone when asked how a no-drone-zone policy for drones could be applied to residential areas.
T1		C17	Technological implementations	30	P1, P2, P4, P7, P9, P10, and P12 shared a number of controls and solutions they felt could be implemented to secure web-enabled cyber devices from drones flying around their homes: Altitude restrictions, time of flight restrictions, distance from home restrictions, laws and policies to protect privacy from drones, some form of jamming device, encryption of personal traffic.

Them e#	Theme Name	Category #	Category Title	Question #	Participant Remarks
T2	Laws, Policies, Law Enforcement, Fines, Notifications, and Reporting	C02	Cybersecurity Policies	30	P1, P2, P4, P7, P9, P10, and P12 shared a number of controls and solutions they felt could be implemented to secure web-enabled cyber devices from drones flying around their homes: Altitude restrictions, time of flight restrictions, distance from home restrictions, laws and policies to protect privacy from drones, some form of jamming device, encryption of personal traffic.
T2		C02	Cybersecurity Policies	27	P4 through P7, and P10 through P14 were not aware of any Anne Arundel County or local cybersecurity or wireless policy that regulated the flying of drones in residential areas.
T2		C02	Cybersecurity Policies	27	P1 and P2 noted their knowledge of drone registration requirements and flight restrictions, but did not state they were aware of any Anne Arundel County or local cybersecurity or wireless policies that regulated flying of drones in residential areas.
T2		C02	Cybersecurity Policies	27	P3, P8, and P9 noted their knowledge of no-fly zones around airports, but did not state they were aware of any Anne Arundel County or local cybersecurity or wireless policies that regulated flying of drones in residential areas.
T2		C02	Cybersecurity Policies	28	P1, P3 through P8, and P10 through P14 were not aware of any Maryland cybersecurity or wireless policy that regulated the flying of drones in residential areas.
T2		C02	Cybersecurity Policies	29	P2, P4 through P8, and P12 through P14 were not aware of any federal cybersecurity or wireless policy that regulated the flying of drones in residential areas.
T2		C02	Cybersecurity Policies	29	P1, P3, P9, P10, and P11 noted their knowledge of drone registration requirements or flight restrictions (e.g. void from airports) and knew there were federal regulations. P3 mentioned an FAA article that identified operational limits for UAS', however; the article did not state it regulated flying of drones in

Them e#	Theme Name	Category #	Category Title	Question #	Participant Remarks
					residential areas.
T2		C02	Cybersecurity Policies	14	P5, P6, P8, P11, P13, and P14 were not sure if there could be any wireless policy that could be implemented to ensure web-enabled cyber devices were not intruded when there was a drone flying around their homes.
T2		C02	Cybersecurity policies	30	P3 felt nothing could be implemented to ensure web-enabled cyber devices were not intruded when there was a drone flying around his home.
T2		C08	Fines	23	P5 felt fines and jail time could be a deterrent to unwanted capture of wireless signals when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.
T2		C08	Fines	38	P1, P2, P4, P5, P6, P7, and P9 through P14 indicated fines ranging from $300-$25,000 should be imposed on operators when their drone attempted to connect to residential cyber/wireless devices when asked what was considered to be a reasonable fine to impose on operators when their drone attempted to connect to residential cyber/wireless devices.
T2		C08	Fines	38	P1, P2, P5, and P6 indicated they wanted law changes, anonymous reporting, and penalties as a result of this study when asked what they you expected from the results of this study.
T2		C08	Fines	34	P3 and P8 indicated no fines should be imposed on operators when their drone attempted to connect to residential cyber/wireless devices when asked what was considered to be a reasonable fine to impose on operators when their drone attempted to connect to residential cyber/wireless devices.
T2		C09	Law	27	P4 through P7, and P10 through P14 were not aware of any Anne Arundel County or local cybersecurity or wireless policy that regulated the flying of drones in residential areas.

Them e#	Theme Name	Category #	Category Title	Question #	Participant Remarks
T2		C09	Law	27	P1 and P2 noted their knowledge of drone registration requirements and flight restrictions, but did not state they were aware of any Anne Arundel County or local cybersecurity or wireless policies that regulated flying of drones in residential areas.
T2		C09	Law	27	P3, P8, and P9 noted their knowledge of no-fly zones around airports, but did not state they were aware of any Anne Arundel County or local cybersecurity or wireless policies that regulated flying of drones in residential areas.
T2		C09	Law	28	P1, P3 through P8, and P10 through P14 were not aware of any Maryland cybersecurity or wireless policy that regulated the flying of drones in residential areas.
T2		C09	Law	28	P2 and P9 noted their knowledge of drone registration requirements and flight restrictions, but did not state they were aware of any Maryland cybersecurity or wireless policies that regulated flying of drones in residential areas.
T2		C09	Law	29	P1, P3, P9, P10, and P11 noted their knowledge of drone registration requirements or flight restrictions (e.g. void from airports) and knew there were federal regulations. P3 mentioned an FAA article identified operational limits for UAS', however; the article did not state it regulated flying of drones in residential areas.
T2		C09	Law	30	P5, P6, P8, P11, P13, and P14 were not sure if there could be any wireless policy that could be implemented to ensure web-enabled cyber devices were not intruded when there was a drone flying around their homes.
T2		C09	Law	30	P3 felt that nothing could be implemented to ensure web-enabled cyber devices were not intruded when there was a drone flying around his home.

Them e#	Theme Name	Category #	Category Title	Question #	Participant Remarks
T2		C09	Law	31	The majority of respondents (P1, P3, P4, P6 through P9, and P11 through P13) overwhelming felt they knew of nothing that could be done to address law enforcement’s handling of drones flown in residential area.
T2		C09	Law	31	P2 indicated drone use could be useful in surveillance and thought there could be laws to address law enforcement’s handling of drones flown in residential areas.
T2		C09	Law	31	P5 indicated there were restrictions, but did not state what restrictions and felt little could be done to address law enforcement’s handling of drones flown in residential areas.
T2		C09	Law	31	P10 indicated drones had been shot down by law enforcement, but did not state where or when; also, P10 felt something could be done to stop drones, but did not state what when asked what they knew about law enforcement’s handling of drones flown in residential areas.
T2		C09	Law	36	P1, P4, and P10 felt law enforcement or another local authority and not a homeowner’s association should address the flying of drones and any attempt to connect to residential cyber devices within residential neighborhoods.
T2		C09	Law	36	P2, P3, P5, and P9 thought enforcement would be an issue even if homeowner associations addressed flying drones to connect to residential cyber devices within residential neighborhoods.
T2		C09	Law	36	P6, P8, P11, P12, and P13 noted they were unsure, there had never been an issue, or the subject had never been brought up at their homeowner's association that addressed flying drones in their neighborhood.
T2		C09	Law	36	P7 and P14 seemed to think the homeowner’s association should discuss addressing flying drones to connect to residential cyber devices within their neighborhood.

Them e#	Theme Name	Category #	Category Title	Question #	Participant Remarks
T2		C09	Law	23	P6, P8, P11, P12, and P13 felt they could offer any idea on blocking or jamming of undesirable drones from capturing wireless signals when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.
T2		C09	Law	23	P1 considered a system shutdown to appropriately block the activity when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.
T2		C09	Law	23	P2 and P14 shared a direct technological solution by jamming when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.
T2		C09	Law	23	P3 indicated collection wireless signals from residential areas couldn’t be stopped when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.
T2		C09	Law	23	P4 offered an encryption solution to ward off the unwanted capture of wireless signals when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.
T2		C09	Law	23	P5 felt fines and jail time could be a deterrent to unwanted capture of wireless signals when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.
T2		C09	Law	23	P7 indicated handling of unwanted capture of wireless signals could be through policy when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.

Them e#	Theme Name	Category #	Category Title	Question #	Participant Remarks
T2		C09	Law	23	P8 noted the handling was dependent on service provider-defined terms on their policy to address unwanted capture of wireless signals when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.
T2		C09	Law	23	P10 offered a technological approach through monitoring since it was noted such wireless capture could not be prevented when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.
T2		C09	Law	38	P1, P2, P5, and P6 indicated they wanted law changes, anonymous reporting, and penalties as a result of this study when asked what they you expected from the results of this study.
T2		C09	Law	33	P5 felt neighborly notifications and approvals must be obtained; otherwise, it would be a no-drone-zone policy for drones in residential areas when asked how a no-drone-zone policy for drones could be applied to residential areas.
T2		C09	Law	17	With the exception of P3, all respondents felt it illegal or a violation of their privacy when drones entered their private spaces, accessed their cyber/wireless devices, created data about them, and placed that data in a cloud; respondents also cringed at the thought of their information collected without their knowledge and placed in some unknown location. Participant #3 responded in an elite manner highly educated in cybersecurity and drones that felt protection of cyber devices, privacy, or otherwise, were that of the homeowner.

Them e#	Theme Name	Category #	Category Title	Question #	Participant Remarks
T2		C09	Law	30	P1, P2, P4, P7, P9, P10, and P12 shared a number of controls and solutions they felt could be implemented to secure web-enabled cyber devices from drones flying around their homes: Altitude restrictions, time of flight restrictions, distance from home restrictions, laws and policies to protect privacy from drones, some form of jamming device, encryption of personal traffic.
T2		C10	Law enforcement	31	The majority of respondents (P1, P3, P4, P6 through P9, and P11 through P13) overwhelming felt they knew of nothing could be done to address law enforcement's handling of drones flown in residential area.
T2		C10	Law Enforcement	31	P2 indicated drone use could be useful in surveillance and thought there could be laws to address law enforcement's handling of drones flown in residential areas.
T2		C10	Law enforcement	31	P5 indicated there were restrictions, but did not state what restrictions and felt little could be done to address law enforcement's handling of drones flown in residential areas.
T2		C10	Law enforcement	31	P10 indicated drones had been shot down by law enforcement, but did not state where or when; also, P10 felt something could be done to stop drones, but did not state what when asked what they knew about law enforcement's handling of drones flown in residential areas.
T2		C10	Law enforcement	36	P1, P4, and P10 felt law enforcement or another local authority and not a homeowner's association should address the flying of drones and any attempt to connect to residential cyber devices within residential neighborhoods.
T2		C10	Law enforcement	36	P2, P3, P5, and P9 thought enforcement would be an issue even if homeowner associations addressed flying drones to connect to residential cyber devices within residential neighborhoods.
T2		C10	Law enforcement	36	P6, P8, P11, P12, and P13 noted they were unsure, there had never been an issue, or that the subject had never been brought up at

Theme#	Theme Name	Category #	Category Title	Question #	Participant Remarks
					their homeowner's association that addressed flying drones in their neighborhood.
T2		C10	Law enforcement	36	P7 and P14 seemed to think the homeowner's association should discuss addressing flying drones to connect to residential cyber devices within their neighborhood.
T2		C11	Notifications	20	P6, P8, P13, and P14 had no idea of whom they would call if they suspected unauthorized activity on their cyber/wireless devices when asked who they would call or notify if they suspected unauthorized activity (e.g. unauthorized surveillance or possible electronic ransom) on any of their cyber/wireless devices in their home and why they selected that person.
T2		C11	Notifications	20	P2, P4, P5, P7, P10, and P11 indicated they would contact a law agency, such as the police or FBI, or the Internet Service Provider for suspected unauthorized cyber/wireless activities; although P5 also indicated he had enough knowledge to take care of the problem when asked who they would call or notify if they suspected unauthorized activity (e.g. unauthorized surveillance or possible electronic ransom) on any of their cyber/wireless devices in their home and why they selected that person.
T2		C11	Notifications	20	P1 would contact a federal governing agency, such as FCC or FAA; P3 and P12 would handle the situation themselves; and P9 would alert whoever was affected during the breach and notify the service provider when asked who they would call or notify if they suspected unauthorized activity (e.g. unauthorized surveillance or possible electronic ransom) on any of their cyber/wireless devices in their home and why they selected that person.
T2		C12	Permission	23	P6, P8, P11, P12, and P13 felt they could offer any idea on blocking or jamming of undesirable drones from capturing wireless signals when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.

Them e#	Theme Name	Category #	Category Title	Question #	Participant Remarks
T2		C12	Permission	23	P1 considered a system shutdown to appropriately block the activity when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.
T2		C12	Permission	23	P2 and P14 shared a direct technological solution by jamming when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.
T2		C12	Permission	23	P3 indicated collection wireless signals from residential areas couldn't be stopped when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.
T2		C12	Permission	23	P4 offered an encryption solution to ward off the unwanted capture of wireless signals when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.
T2		C12	Permission	23	P5 felt fines and jail time could be a deterrent to unwanted capture of wireless signals when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.
T2		C12	Permission	23	P7 indicated handling of unwanted capture of wireless signals could be through policy when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.
T2		C12	Permission	23	P8 noted the handling was dependent on service provider-defined terms on their policy to address unwanted capture of wireless signals when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.

Them e#	Theme Name	Category #	Category Title	Question #	Participant Remarks
T2		C12	Permission	23	P10 offered a technological approach through monitoring since it was noted such wireless capture could not be prevented when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.
T2		C12	Permission	17	With the exception of P3, all respondents felt it illegal or a violation of their privacy when drones entered their private spaces, accessed their cyber/wireless devices, created data about them, and placed that data in a cloud; respondents also cringed at the thought of their information collected without their knowledge and placed in some unknown location. Participant #3 responded in an elite manner highly educated in cybersecurity and drones felt protection of cyber devices, privacy, or otherwise, were responsibilities of the homeowner.
T2		C12	Permission	21	P5, P6, P7, P9, and P13 were altogether unsure of any action their service providers could take remotely to control their cyber/wireless devices when asked what cyber/wireless device and what actions their provider could take to remotely control their device without their permission or knowledge.
T2		C12	Permission	21	Respondents P1-P4, P10-P12, and P14 all indicated their service providers could remotely perform updates or some action to their cyber devices without the participants' knowledge when asked what cyber/wireless device and what actions their provider could take to remotely control their device without their permission or knowledge.
T2		C13	Policies	23	P7 indicated handling of unwanted capture of wireless signals could be through policy when asked what legal measures they envisioned could be implemented to block or jam unwanted drones from capturing wireless signals from their residence.
T2		C13	Policies	33	P13 felt a petition could be made to address a no-drone-zone policy for drones in residential areas when asked how a no-drone-

Them e#	Theme Name	Category #	Category Title	Question #	Participant Remarks
					zone policy for drones could be applied to residential areas.
T2		C13	Policies	33	P6, P11, and P12 were unsure of how a no-drone-zone policy for drones could be applied to residential areas when asked how a no-drone-zone policy for drones could be applied to residential areas.
T2		C13	Policies	33	P1 and P7 felt a no-drone-zone policy could be applied to residential areas, but did not state how when asked how a no-drone-zone policy for drones could be applied to residential areas.
T2		C13	Policies	33	P2 and P8 felt even if there was a no-drone-zone policy for drones in residential areas, it would be difficult to enforce when asked how a no-drone-zone policy for drones could be applied to residential areas.
T2		C13	Policies	33	P4 felt gaining an owner's permission could be applied in a no-drone-zone policy for drones in residential areas when asked how a no-drone-zone policy for drones could be applied to residential areas.
T2		C13	Policies	33	P9 felt no-drone-zone policies for drones could be applied to residential areas as are at airports when asked how a no-drone-zone policy for drones could be applied to residential areas.
T2		C13	Policies	33	P5 felt neighborly notifications and approvals must be obtained; otherwise, it would be a no-drone-zone policy for drones in residential areas when asked how a no-drone-zone policy for drones could be applied to residential areas.
T2		C13	Policies	33	P3 felt that jammers could be applied in a no-drone-zone policy for drones in residential areas, but also felt defensive mechanisms could really be the best defense when asked how a no-drone-zone policy for drones could be applied to residential areas.

Them e#	Theme Name	Category #	Category Title	Question #	Participant Remarks
T2		C13	Policies	33	P10 felt a technological solution that integrated residential homes into the drone application could be used to distinguish the homes as a no-drone-zone when asked how a no-drone-zone policy for drones could be applied to residential areas.
T2		C13	Policies	34	P3 and P8 indicated no fines should be imposed on operators when their drone attempted to connect to residential cyber/wireless devices when asked what was considered to be a reasonable fine to impose on operators when their drone attempted to connect to residential cyber/wireless devices.
T2		C14	Privacy	17	With the exception of P3, all respondents felt it illegal or a violation of their privacy when drones entered their private spaces, accessed their cyber/wireless devices, created data about them, and placed that data in a cloud; respondents also cringed at the thought of their information collected without their knowledge and placed in some unknown location. Participant #3 responded in an elite manner highly educated in cybersecurity and drones felt protection of cyber devices, privacy, or otherwise, were responsibilities of the homeowner.
T2		C14	Privacy	32	There were 35.7% of respondents who indicated *5* and felt drones in their residential neighborhood was most invasive, 14.3% rated *4-4.5*, 21.4% rated *3*, 14.3% rated *2*, and 14.3% rated *1* when asked how they would rate drone operations in residential areas.
T2		C15	Remote Access	21	P5, P6, P7, P9, and P13 were altogether unsure of any action their service providers could take remotely to control their cyber/wireless devices when asked what cyber/wireless device and what actions their provider could take to remotely control their device without their permission or knowledge.

Them e#	Theme Name	Category #	Category Title	Question #	Participant Remarks
T2		C15	Remote Access	21	P1-P4, P10-P12, and P14 all indicated their service providers could remotely perform updates or some action to their cyber devices without the participants' knowledge when asked what cyber/wireless device and what actions their provider could take to remotely control their device without their permission or knowledge.
T2		C16	Reporting	38	P1, P2, P5, and P6 indicated they wanted law changes, anonymous reporting, and penalties as a result of this study when asked what they you expected from the results of this study.
T2		C16	Reporting	20	P6, P8, P13, and P14 had no idea of whom they would call if they suspected unauthorized activity on their cyber/wireless devices when asked who they would call or notify if they suspected unauthorized activity (e.g. unauthorized surveillance or possible electronic ransom) on any of their cyber/wireless devices in their home and why they selected that person.
T2		C16	Reporting	20	P2, P4, P5, P7, P10, and P11 indicated they would contact a law agency, such as the police or FBI, or the Internet Service Provider for suspected unauthorized cyber/wireless activities; although P5 also indicated he had enough knowledge to take care of the problem when asked who they would call or notify if they suspected unauthorized activity (e.g. unauthorized surveillance or possible electronic ransom) on any of their cyber/wireless devices in their home and why they selected that person.

Them e#	Theme Name	Category #	Category Title	Question #	Participant Remarks
T2		C16	Reporting	20	P1 would contact a federal governing agency, such as FCC or FAA; P3 and P12 would handle the situation themselves; and P9 would alert whoever was affected during the breach and notify the service provider when asked who they would call or notify if they suspected unauthorized activity (e.g. unauthorized surveillance or possible electronic ransom) on any of their cyber/wireless devices in their home and why they selected that person.

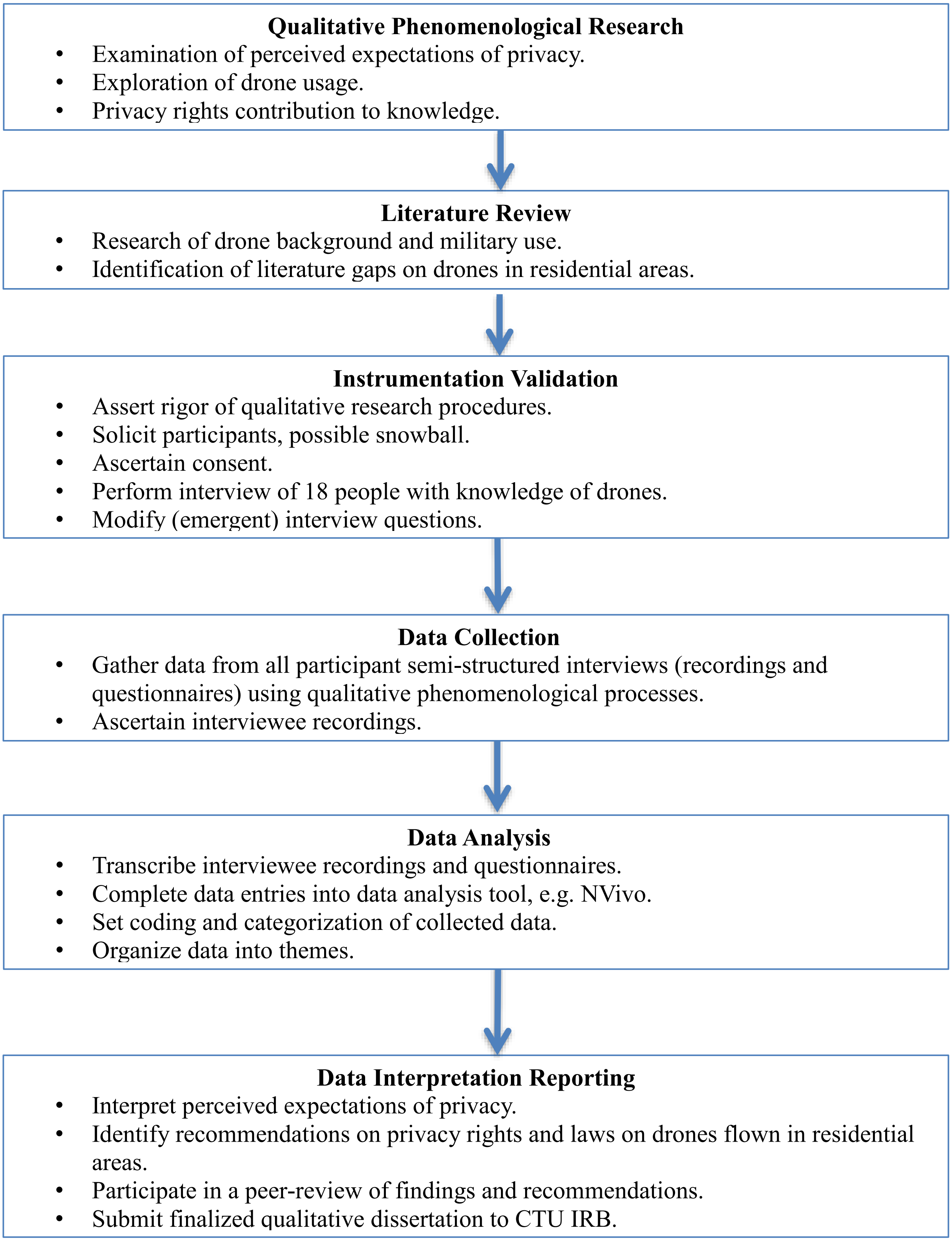
Them e#	Theme Name	Category #	Category Title	Question #	Participant Remarks
T3	Residential education in cybersecurity	C04	Cybersecurity training	37	P6, P8, and P13 were unsure of training deficiencies in cybersecurity in their neighborhood when asked what kind of cybersecurity training they felt was needed for residences to become more knowledgeable of wireless connectivity capabilities with drones flying in residential neighborhoods.
T3		C04	Cybersecurity training	37	P1 through P5, P7, P9 through P12, and P14 desired some form of announcements, notices, education and awareness, informative meetings, and training were needed for residences to become more knowledgeable of wireless connectivity capabilities with drones flying in residential neighborhoods.
T3		C07	Education	13	P6, P7, and P11 considered they knew very little about drones or unmanned aerial systems.
T3		C07	Education	13	P3, P8, and P13 thought they knew a fair amount of information about drones.
T3		C07	Education	13	P1, P2, P4, P5, P9, P10, and P12 felt they were quite knowledgeable and understood uses and capabilities of drones and UAS'.

Them e#	Theme Name	Category #	Category Title	Question #	Participant Remarks
T3		C07	Education	14	P6, P13, and P14 indicated they had no experience with drones or UAVs.
T3		C07	Education	14	P2, P4, P5, and P12 acknowledged one sighting of a drone in neighboring or recreational areas, but no experience.
T3		C07	Education	14	P1, P3, P7, P8, P9, P10, and P11 felt they attained some experience with drones when they witnessed or handled two or more drones. P3 felt quite comfortable with experience gained.
T3		C07	Education	38	P7, P9, P10, and P14 indicated the result of this study should produce more education on security risks with drones and capabilities that could access personal wireless and cyber devices, and about risks and mitigations in cybersecurity when asked what they you expected from the results of this study.
T3		C07	Education	30	P1, P2, P4, P7, P9, P10, and P12 shared a number of controls and solutions they felt could be implemented to secure web-enabled cyber devices from drones flying around their homes: Altitude restrictions, time of flight restrictions, distance from home restrictions, laws and policies to protect privacy from drones, some form of jamming device, encryption of personal traffic.
T3		C07	Education	38	P4 thought the study could produce a great deal of opinions when asked what they you expected from the results of this study.
T3		C07	Education	38	P3 desired to read the dissertation once available when asked what they you expected from the results of this study.

Them e#	Theme Name	Category #	Category Title	Question #	Participant Remarks
T4	Package Deliveries by Drones	C05	Delivery Notifications	25	Although P5 was opposed to deliveries by drones, phone calls could be acceptable if drones made deliveries when asked what notification methods they felt could be used to make wireless deliveries by drones to their homes acceptable.
T4		C05	Delivery Notifications	25	P1, P6, P13, and P14 were against deliveries by drones when asked what notification methods they felt could be used to make wireless deliveries by drones to their homes acceptable.
T4		C05	Delivery Notifications	25	P2, P3, P4, and P7 through P12 thought electronic notifications through text messages or email were acceptable means prior to deliveries by drones when asked what notification methods they felt could be used to make wireless deliveries by drones to their homes acceptable.
T4		C05	Delivery Notifications	26	P1, P5, P6, P9, and P13 indicated they were totally against drone deliveries to their residences and thought it a bad idea when privacy was jeopardized when asked what notification methods they felt could be used to make wireless deliveries by drones to their homes acceptable.
T4		C05	Delivery Notifications	26	P2, P3, P4, P7, P10, P11, and P12 seemed to be acceptable to the idea of the possibility of giving up on privacy for the capability to have drones deliver packages when asked what notification methods they felt could be used to make wireless deliveries by drones to their homes acceptable.
T4		C06	Drone Package Deliveries	24	P1, P5, P6, P8, P13, and P14 were adamantly opposed to cyber/wireless capabilities for drone package deliveries to residences when asked what they thought about cyber/wireless capabilities to make package deliveries to their residence using drones.
T4		C06	Drone Package Deliveries	24	P2, P3, P4, P7, P9, P10, and P12 were very open and receptive to the concept using cyber/wireless technology to deliver packages by drones when asked what they thought about cyber/wireless capabilities to make package deliveries to their residence using drones.

Them e#	Theme Name	Category #	Category Title	Question #	Participant Remarks
T4		C06	Drone Package Deliveries	14	P11 never considered drones to deliver packages when asked what they thought about cyber/wireless capabilities to make package deliveries to their residence using drones.
T4		C06	Drone Package Deliveries	25	P1, P6, P13, and P14 were against deliveries by drones when asked what notification methods they felt could be used to make wireless deliveries by drones to their homes acceptable.
T4		C06	Drone Package Deliveries	25	Although P5 was opposed to deliveries by drones, phone calls could be acceptable if drones made deliveries when asked what notification methods they felt could be used to make wireless deliveries by drones to their homes acceptable.
T4		C06	Drone Package Deliveries	25	P2, P3, P4, and P7 through P12 thought electronic notifications through text messages or email were acceptable means prior to deliveries by drones when asked what notification methods they felt could be used to make wireless deliveries by drones to their homes acceptable.
T4		C06	Drone Package Deliveries	26	P1, P5, P6, P9, and P13 indicated they were totally against drone deliveries to their residences and thought it a bad idea when privacy was jeopardized when asked what notification methods they felt could be used to make wireless deliveries by drones to their homes acceptable.
T4		C06	Drone Package Deliveries	26	P2, P3, P4, P7, P10, P11, and P12 seemed to be acceptable to the idea of the possibility of giving up on privacy for the capability to have drones deliver packages when asked what notification methods they felt could be used to make wireless deliveries by drones to their homes acceptable.

Appendix E: Methodology Map



Qualitative Phenomenological Research

- Examination of perceived expectations of privacy.
- Exploration of drone usage.
- Privacy rights contribution to knowledge.

Literature Review

- Research of drone background and military use.
- Identification of literature gaps on drones in residential areas.

Instrumentation Validation

- Assert rigor of qualitative research procedures.
- Solicit participants, possible snowball.
- Ascertain consent.
- Perform interview of 18 people with knowledge of drones.
- Modify (emergent) interview questions.

Data Collection

- Gather data from all participant semi-structured interviews (recordings and questionnaires) using qualitative phenomenological processes.
- Ascertain interviewee recordings.

Data Analysis

- Transcribe interviewee recordings and questionnaires.
- Complete data entries into data analysis tool, e.g. NVivo.
- Set coding and categorization of collected data.
- Organize data into themes.

Data Interpretation Reporting

- Interpret perceived expectations of privacy.
- Identify recommendations on privacy rights and laws on drones flown in residential areas.
- Participate in a peer-review of findings and recommendations.
- Submit finalized qualitative dissertation to CTU IRB.

Figure 1: Methodology Map