Privacy Under Pressure: A Survey of Privacy Expectations in the Modern Age

by

James Easton Horton

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Criminal Justice

Middle Tennessee State University

May 2018

Advised By:

Dr. Lance Selva, Thesis Chair

Dr. Joshua Harms, Reader and Data Analysis

J.D. William Shulman, Reader

ABSTRACT

Cell site location information (CSLI) data is currently on the forefront of the privacy law debate but remains unresolved and unregulated by the judiciary. In accordance with the second prong of the *Katz* test, public perception is vital in resolving the legal contest surrounding CSLI. This study examines the privacy expectations of 1320 college students at Middle Tennessee State University. A privacy scale was created from 1 to 72. The higher the score, the higher the privacy expectation. This study found that men tend to have stronger privacy expectations than women by 1.83 points on average. African Americans were found to have the highest expectation of privacy at 48.44, while Asians reported the lowest at 43.78. Privacy expectation was positively correlated with age although the correlation is weak (R=.115). Overall, respondents held high privacy expectations regardless of demographic factors. All tests were found to be statistically significant.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER I

INTRODUCTION

Statement of the Hypothesis

It is hypothesized that the variables of sex, race, and age will all have measurable variations of their respective privacy scores. It is posited that men will have higher privacy expectations than females; members of minority groups will have lower privacy expectations than members of majority groups; and that as the age of the respondent increases, their respective privacy expectations will also increase. Furthermore, the researcher posits that despite variations in privacy expectation, the overall privacy expectation will remain high across all variables, mirroring studies that were similar in nature.

Statement of the Problem

The right of privacy is of special significance to American society. According to the Pew Research Center, a substantial portion of Americans have stated that there is a significant public interest in government interference of privacy (Madden and Rainie, 2015). Privacy is at the forefront of legal litigation and poses a unique challenge to the courts, as solving the issue entails the reassessment of the relationship between modern technology and privacy.

The struggle between technology and privacy law is not confined to the modern historical period. Significant changes have been made in relation to privacy expectations since the inception of the Fourth Amendment, which serves as the constitutional underpinning of the liberty interest in the Due Process Clause (Walsh, 2012, pp.171-173). The U.S. Supreme Court has overcome these jurisprudential issues by evolving new legal

systems that serve as protection against the advancement of technology (Donohue, 2017, pp. 581-640).

Today, this privacy debate is inculcated in the issues of cell cite location information (CSLI) tracking. Using CSLI, law enforcement has the ability to intercept a cell phone's essential communications with the cellular tower. These signals can then be triangulated using various methodologies to determine a precise location of an individual's cellular device. This allows for law enforcement to monitor an individual's movements with little effort and cost (Wallentine, 2011, pp.403-406). Furthermore, in its current state, CSLI technology remains virtually unregulated and requires the Court to reevaluate protections and establish new systems that shield citizens from potential Fourth Amendment violations (Burten, 2012, pp. 371-375)

In solving this legal conflict, the Court relies heavily on the *Katz* test, which is a bifurcated legal questioning process which determines whether Fourth Amendment protections apply to an action taken by the government. The first prong focuses on the subjective expectation of privacy the individual possessed and the second prong examines the objective expectation of privacy that society in large holds as reasonable (*Katz v US*, 1967, pp. 4-5). While a great deal of legal precedent and jurisprudence has been established on the subjective prong of the *Katz* test, there is a noticeable gap in empirical measurements of the objective privacy expectations of society at large (Slobogin, 2011, pp.4). This knowledge gap hinders the ability of the judicial system to make assessments concerning the public's objective expectation of privacy. In order to achieve these measurements, empirical data must be collected that measures these objective privacy expectations.

Purpose of the Study

In the seminal case of *United States v Jones* (2012), Supreme Court Justice Sotomayor states: "The same technological advances that have made possible nontrespassory surveillance techniques will also affect the *Katz* test by shaping the evolution of societal privacy expectations." (*United States v Jones*, 2012, pp.14-15). This study was designed with the intention of demonstrating the quantitative value of the expectation of privacy of college students at Middle Tennessee State University. The data gathered by this study will provide quantitative information on the interaction between variables and their respective privacy expectations. The variables measured are sex, race, and age. The results of these measurements will aid in the efforts of the courts and the criminal justice community to answer the second prong of the *Katz* test and to suggest an objective and quantifiable basis for assessing society's privacy expectations. The data collected can also be utilized to draw comparisons with previous studies of a similar nature and will possibly demonstrate developing trends in privacy expectations nationwide.

Scope of the Study

This study involves the measurement of the responses of 1276 students of Middle Tennessee State University. This population was selected as students of this age range were believed to be frequent users of cellular phones, computers, and social media on a consistent basis. The target population was cellular phone users who were students at Middle Tennessee State University. The sampling frame for this study was an availability sample. A survey was utilized which was designed to gauge their respective expectations of privacy in relation to law enforcement's utilization of advanced tracking technology.

This study was conducted in three waves from the years 2012-2017. This study is the application and analysis of the third and final wave of this study, as well as an analysis of all previous waves.

CHAPTER II

REVIEW OF LITERATURE

Overview of CSLI Technology

CSLI tracking is an interception of a cellular phone's wireless functioning processes. When a cell phone is activated, a process called registration initiates (Harkins, 2011). During this process, the cellular phone emits a signal which travels to the nearest provider tower in order to open a connection for correspondence such as text messages and phone calls. The process of registration completes approximately every seven seconds (Curtiss, 2011, p.848). While this process may seem innocuous, it serves as a vigilant autonomous tracking methodology over a general geographical area for anyone who has the proper equipment to intercept these cellular emissions. In order to gain a more precise location of a cellular device, wireless service providers employ two other methods of determining location. These are called Time Distance of Arrival (TDOA) and Angle of Arrival (AOA) (Selva, Shulman & Rumsey, 2016, pp. 239-240). With TDOA, multiple cellular towers receive the signal from the cellular phone then convert the time differential into a triangulation measurement. With AOA, a similar method is employed except the angle at which the registration arrives is the measurement of triangulation rather than the time differential (Selva, et al, 2016, p. 239).

Law enforcement actively use this information, by interception of these signals, in order to preform continuous, location-based surveillance on a potential suspect (Dennis, 2011). In the year 2011 alone, records reveal that wireless service providers received 1.3 million requests for cellular location information (Lichblau, 2012). These requests can be subdivided into two general types: historical and active or "real time" (Harkins, 2011).

Historical CSLI allows law enforcement to view the history of a particular cellular device's registration process at a particular date and time. Active CSLI, allows law enforcement to monitor the current location of a cellular device in real time (Bennardo, 2017, pp. 2391-2393). Law enforcement can take this data and construct a highly precise location of the cellular device, and by extension, the owner of the device.

Judicial Precedents in Privacy and Technology

From a historical standpoint, privacy law in the United States is frequently shaped around the emergence of new technologies (*Katz v US*, 1967; *Knotts v US*, 1983; *Karo v US*, 1984; *Kyllo v US*, 2001). Before the seminal case of *Katz v US* (1967), ideas of privacy and Fourth Amendment protections were coupled to the legal distinction between public and private property. Private property has, historically, been given a higher degree of Fourth Amendment protection. In public, privacy expectations were virtually nonexistent due to expectations of privacy resting almost solely on the basis of property (Colb, 2004). However, these legal precepts were challenged in the 1967 case *Katz v US*, in which the defendant's private telephone conversation was monitored from the outside of a public phone booth (*Katz v US*, 7967, p.1). The government argued this was public property thus no expectation of privacy existed at the time of the recording (*Katz v US*, 1967, p.2). The decision of the *Katz* case was twofold. Firstly, it decoupled the concept of privacy and property, which extended Constitutional protections to individuals in public as well as private property. Secondly, it led to the creation of a bifurcated legal questioning process that would serve as a legal mechanism to determine if an action taken by authorities qualified as a Fourth Amendment search (*Katz v US*, 1967, pp.5-6). This process posed two primary questions. Firstly, does the individual exhibit a reasonable

expectation of privacy. Secondly, does society recognize that expectation as reasonable (*Katz v US*, 1967, pp.6). The two-pronged test in *Katz* was accepted as the penultimate test for determining the extension of Fourth Amendment protections and is still utilized in the Court's deliberation and jurisprudence (Walsh, 2012, 185-187).

As time progressed, new technologies were developed that again challenged privacy rights. In the 1980s, *US v Knotts* (1983) stands out as a case of salience and plays a significant role in establishing the foundational arguments that are used for CSLI tracking today. *US v Knotts* (1983) involved a situation in which the authorities placed an electronic location monitor inside a barrel of chemicals that was being used to manufacture illegal drugs (*US v Knotts*, 1983, p.3). Investigators tracked the signal of the beeper that was placed in the barrel on open highways to its eventual storage location. When brought before the Supreme Court, the Court established that police utilization of sensory enhancing technologies was not prohibited by the Fourth Amendment (*US v Knotts*, 1983, p.5). This decision was reached on the premise that since the barrel was being transported on a public highway, there could be no expectation of privacy, which failed the first prong of the *Katz* test. The precedent that *Knotts* established was twofold: firstly, individuals traveling on open roads cannot pass the first prong of the *Katz* test as there is no reasonable expectation of privacy and thus individuals are not protected by the Fourth Amendment. Secondly, that the use of sensory enhancing technology such as tracking devices does not constitute a breach of Fourth Amendment protections as the tracking did not create a scenario that could not be done physically, it simply enhanced the investigator's ability to track the target in a public venue (*US v Knotts*, 1983, p.460)

Following the decision in *Knotts*, the legality of beeper tracking methods was modified in the landmark case of *Karo v US* (1983). In this case DEA agents placed an electronic tracking device inside a barrel of ether that was being purchased by a suspected drug manufacturer (*Karo v US*, 1984, p.468). The barrel was tracked to various residences and was eventually seized by law enforcement at the residence of the defendant (pp. 468-469). When challenged in lower courts, the monitoring of the beeper was not considered a breach of Fourth Amendment protections on the basis of the decision in *Knotts* (1983). When reviewed by the Supreme Court, issue was taken with the monitoring of the tracking device on private property and attaining information from inside a private residence (pp. 713-718). The Court found that gathering information emanating from a private residence was substantively different than that of tracking on public roadways (pp.719-721). This decision modified the decision made in *Knotts* and created a legal differentiation between information obtained on public roadways and information emanating from a private residence (pp.721).

Another case that contributes significantly to the current CSLI argument is *Kyllo v US* (2001). The *Kyllo* case questions the legality of nonphysical trespass through the use of advance of technology. In *Kyllo*, law enforcement personnel utilized a thermal imaging device to detect heat signatures through the walls of the defendant's home (p.27). When a large, abnormal heat signature was detected the officers determined that it was likely home to a marijuana grow operation and subsequently raided the defendant's home, leading to his arrest. The Court was again faced with a legal decision in which Fourth Amendment protections were challenged by advance technology. In its ruling, the Court curbed the previous rulings regarding sensory enhancing technology that was established

in the *Knotts* case. The Court established a new policy which concludes that if a Fourth Amendment violation would have occurred in the process of gathering the information in question through unaided means, a warrant is required to utilize the technology (*Kyllo v US*, 2001, p. 30). In his opinion, Justice Scalia noted that the expectation of privacy within the home extended to the heat emissions observed by the thermal imager and that surveillance conducted "off the wall" was the same as "through the wall" for the purposes of Fourth Amendment protections (*Kyllo v US*, 2001, pp.31-33)

Recently, the Supreme Court confronted privacy questions concerning cellular phones more directly in the landmark case *Riley v California* (2014). In this case, the suspect was arrested for weapons charges related to a search of his vehicle at a traffic stop. In the search incident to arrest, Riley's cell phone was seized and searched by officers (*Riley v California*, 2014, p.1). Officers discovered communications with known gang members as well as evidence that Riley was involved in gangland criminal activity. In the trial court, Riley moved to suppress the evidence on the cell phone but the suppression was denied and the case was appealed to the Supreme Court. The Court held that police may not search the contents of a cellular phone incident to arrest without a warrant under normal circumstances as per the precedent established in *Chimel v California,* (1969). In *Chimel* the Court concluded that search incident to arrest was limited in scope to areas where the suspect could potentially obtain a weapon or attempt to destroy evidence (*Chimel v California*, 1969, pp.8). More importantly, the Court stated that the privacy interest pertaining to information on a cellular phone holds a much more substantial privacy interest than a brief search of the arrestee and the space they occupy (*Riley v California*, 2014, pp. 2). Further expounding on this, the *Riley* Court stated that

the government's interest in preserving and discovering data on the cellular phone does not outweigh the privacy interest of the arrestee (*Riley v California*, 2014, pp.2-3)

Technology has been at odds with privacy interests historically and has raised new legal issues for the courts to address (McLaughlin, 2007, pp.422-423). The Supreme Court has frequently recognized a need to modernize privacy laws as technology has grown more advanced and invasive. The establishment of the *Katz* test decoupled the trespass doctrines of old and fostered protections for individuals in public. The Court has also taken vital steps in attempting to insulate privacy rights from emergent technology (*Katz v US*, 1967; *US v Knotts*, 1983; *US v Karo*, 1984; *US v Kyllo*, 2001; *US v Jones*, 2012; *Riley v California*, 2014). The Court has relied heavily on judicial precedent in navigating the boundary between privacy and modern technology (Harkins, 2011, pp.1885-1887). This boundary is currently being challenged by CSLI and many scholars argue it is due for the Court's consideration (Harkins, 2011, p.1919; Hutchins, 2011, p.495; Ford, 2007, p.1370)

The Current Regulation of CSLI

CSLI technology is currently shrouded in a state of legal limbo. The technology of CSLI is still in a state of legal infancy and is only controlled through crude statutes and regulations (Chamberlain, 2004). Currently, CSLI is controlled through a rough amalgamation of specific sections of the Electronic Communications Privacy Act (ECPA) and, more specifically, the second and third portions of the ECAP known colloquially as the Stored Communications Act (SCA). These two portions of the ECPA allow for the disclosure of electronic communications provided that law enforcement provide reasonable suspicion that these communications are relevant and material to an

ongoing investigation (Freiwald, 2011, pp.738-742). The utilization of the ECPA in this manner has been hotly debated in various cases across multiple levels of the judicial system (*US v Maynard*, 2010; *US v Jones*, 2012; *Carpenter v US*, 2016; *Graham v US*, 2016). Despite this legal contest, no formal decisions have prevented the government from utilizing CSLI technology or establishing a warrant requirement to operate a CSLI operation on a national level.

The government's legal justification for the utilization of CSLI has been argued from the voluntary disclosure precedents established in the *Knotts* case and the third-party doctrine (Ostrander, 2011, pp.1759-1765). The government argues that location information is considered voluntarily disclosed when the individual is in public. This standard would trigger a failing of the first prong of the *Katz* test rendering the suspect's actions unprotected by the Fourth Amendment (Hutchins, 2007). This philosophy supposes CSLI to be a natural extension of the beeper tracking cases and is, therefore, governed by those same legal standards. The standards established by *Knotts* holds that a reasonable expectation of privacy cannot be established as the individual is knowingly exposing their movements to the public (*US v Knotts*, 1983).

The government also provides legal justification for the interception of cellular signals via the third-party doctrine. This doctrine was formed from the Supreme Court decisions in the cases *Smith v Maryland* (1979) and *United States v Miller* (1976). In these cases, the Supreme Court established a doctrine which concluded that an individual cannot be extended Fourth Amendment protections on information that is willingly disclosed to a third party (*Smith v Maryland*, 1979, pp.4-8). The *Miller* Court, in a case

where bank records of a customer were used to establish evidence of criminality, stated the following:

> "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." (*United States v Miller*, 1976, pp. 441-443)

The government, in the case of CSLI tracking, simply extends the same argument to the location information that is being shared through the registration process of a cellular device. In order for the device to function, registration must be established. Therefore, the government argues that individuals who voluntarily choose to use a cell phone cannot have a legal expectation of privacy that extends to the communications that they share with their wireless provider, a third party (R.H.M, 1985, pp.310-314).

Judicial response to the government's argument has been varied and frequently conflicts at multiple levels of the judicial system (Hutchins, 2007, pp.445-452). Currently, there have been three Federal Court rulings, four State Court rulings and one Supreme Court ruling concerning GPS based tracking (Hutchins, 2007, pp.445). Of these cases, only two offer worthwhile commentary on the actual privacy implications of GPS tracking; *Washington v Jackson* (2003) and *US v Jones* (2012). In *Washington v Jackson* (2003), the Court considered the government's position on two primary issues: the sensory enhancement argument and the use of the *Knotts* precedent as justification for the

tracking. Speaking of the sensory enhancement argument, the Court stated: "Unlike binoculars or a flashlight, the GPS device does not merely augment an officer's senses but rather provides a technological substitute for traditional tracking." (*Washington v Jackson*, 2003, p. 32) The *Jackson* Court also stated: "in this age, vehicles are used to take people to a vast number of places that can reveal preferences, alignments, associations, personal ails and foibles." (*Washington v Jackson*, 2003, p. 34). The Court concluded that GPS tracking was of a more intrusive nature than that of traditional surveillance or beeper tracking. This higher degree of intrusiveness coupled with the increased quantity of information collected led the Court to recommend that a higher requirement than reasonable suspicion be the controlling standard (*Washington v Jackson*, 2003; Hutchins, 2007).

In *US vs Jones* (2012), questions concerning GPS tracking were largely avoided due to the Court finding a trespass in the placement of the tracking device on Jones' vehicle causing the case to be dismissed (*US v Jones*, 2012). However, several vital remarks were made in the Justice's opinions, especially in the concurring opinions of Justice Alito and Justice Sotomayor. In the *Jones* case, the defendant was monitored via a GPS tracking device that was placed under his vehicle. This tracking device was monitored constantly for a period of twenty-eight days. Justice Alito noted that there seemed to be an intrinsic difference between short-term surveillance and long-term surveillance and established this distinction as the difference between a suspect being observed in a singular incident and a suspect being continually watched for a protracted period of time (*US v Jones*, 2012, pp.7). Additionally, he noted that a citizen would not expect a to be monitored on a continual basis by a member of the public. However, he

avoided specifying the specific time determination of what constituted "surveillance that was too intrusive" from that which was not (*U.S. v Jones*, 2012, p.8).

Justice Sotomayor concurred with Justice Alito in finding that the protracted tracking period, as seen in *Jones*, would likely intrude on society's normative expectations of privacy (p.11-12). However, she extends the conversation further, even suggesting that Justice Alito's opinion "suffices to decide this case" (p. 12). She makes the argument that this type of GPS tracking allows the government to obtain a much clearer picture of an individual's private dealings than what would be expected by a normal citizen. She specifically states:

> "I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on? I do not regard as dispositive of the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques." (*US v Jones*, 2012, p.18)

In addition, she proposes that this type of monitoring will shape privacy expectations in the future and argues that these new tracking technologies suffer from two primary problems. First, these technologies have the potential to provide a massive wealth of personal information on the target of the investigation (*US v Jones*, 2012, pp.17). This information, in many cases, would not necessarily be pertinent to the investigation. Further, such tracking creates an extremely broad scope of aggregated information, from visits to the doctor to religious preferences (*US v Jones*, 2012, pp.17-18). In the opinion of Sotomayor, the government's utilization of the *Knotts*' precedent,

in which an individual can have no expectation of privacy regarding movement that is in open view of the public, does not satisfy a scenario of autonomous, ever-present tracking. Secondly, Justice Sotomayor suggests that the third-party doctrine is ill suited for this new age of digital technology (*US v Jones,* 2012, p. 19). In this age, individuals are often required to share information with third parties in order to utilize the service. Should such utilization of a service necessarily suspend Fourth Amendment protections? In reply, Justice Sotomayor quotes the *Katz* case, stating: "What a person seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected" (*Katz v US*, 1967, p. 351-352).

Legal scholars have examined the opinion of Justice Sotomayor and believe that it is the initiation of a new jurisprudence concerning privacy in the digital age (Elgart, 2016, pp.634-636). This new jurisprudence places legal significance on the volume and intrusiveness of the information that was collected rather than focusing solely on the methodology and execution of the collection of the data. Scholars have argued that this new jurisprudence is commonly referred to as a "mosaic shield" which protects individuals from surveillance methodologies that collect aggregate data (Dennis, 2011, pp.763-767). The theory states that by the aggregation of a mass amount of data points from prolonged surveillance, an individual is susceptible to dragnet surveillance that paints a very intimate picture of an individual's life which extends beyond the scope of what is being investigated. Some argue that the mosaic shield theory may serve as a flexible augmentation of the existing *Katz* standards that better suit these new surveillance methods for the digital age (Ford, 2011, pp.1354; Dennis, 2011, pp.760).

Prior Research on the Public Expectation of Privacy

The Supreme Court in *US v Jones* acknowledged a knowledge gap concerning a quantifiable measurement of the public's privacy expectations (*US v Jones*, 2012, p.20). This same question had been considered by scholars for quite some time but no solid empirical measurements had been conducted (Slobogin and Schumacher, 1993). This deficit was addressed by more modern studies that sought to put a numerical measurement to the question of privacy expectations. These studies hoped these measurements would substantially inform the second prong of the *Katz* test. This would allow the court to further its decision making concerning privacy rights with well-informed studies supporting the decision (Kerr, 2012)

Christopher Slobogin's *Privacy at Risk* (2011) is among the first of these studies that sought to establish a foundation for empirical examination of the public's expectation of privacy. In the study, Slobogin polled jury pools and asked for respondents to rate government search actions on a scale from less intrusive to more intrusive. He found that, under most circumstances, the average expectation of privacy aligned closely with existing law and court rulings. However, in some situations, such as the use of an undercover informant, the average individual rated the methodology as extremely intrusive despite the action being less regulated by the court. Overall, Slobogin's study served, despite flaws, to introduce the concept of empirical measurement of privacy expectations. The most significant weakness of the Slobogin study was the utilization of a jury pool as subjects. This selection inhibits the ability of the study to gauge an accurate assessment of the average citizen's expectation of privacy on a national scale (Kerr, 2007, pp.961).

Eight years later, Matthew Kugler and Lior Strahilevitz attempted to bridge the gaps in Slobogin's study by launching a nationally weighted study on the average expectation of privacy. The study was divided into three waves. The first wave was designed to measure trends in the expectation of privacy. The second and third waves were designed to probe deeper into the findings of the first wave, particularly in the rationale behind the privacy expectation given in wave one. The final sample size for the survey was 1,461 participants (Kugler and Strahilevitz, 2015, p.246). The study included a vast array of demographics and ages, with the purpose being to create a nationally weighted sample that would address the weaknesses of Slobogin's previous study. The study revealed several significant results. Firstly, a majority of participants in the study found that GPS tracking violated their expectations of privacy. This response was gauged in a series of four questions each referencing a different duration of tracking. In each of the four questions, more than fifty-percent of respondents were above the mid-point in privacy expectations concerning the intrusiveness of the action (Kugler and Strahilevitz, 2015, p.246-247). Essentially, the study found that the length of the government's GPS tracking of an individual plays very little into the individual's expectation of privacy. In fact, the researchers indicated that 81% of respondents gave the same score to tracking over the course of 24 hours and over the course of a month. As Slobogin also found, duration seems to be irrelevant to the question of the intrusiveness of GPS tracking (Slobogin, 2007; Kugler, et. al., 2015, p.248).

In wave two of the study, respondents were asked their reasoning behind their respective privacy responses. Interestingly, respondents who were found to have a low expectation of privacy most commonly cited their rationale as being a derivative of the

third-party doctrine. The rationale being that an individual is sharing their location with the public thus they cannot have a reasonable expectation of privacy regarding their movements (Kugler and Strahilevitz, 2015. p.249-250). Respondents who scored with a high expectation of privacy citied two rationales at almost equal frequency. The first being the potentiality of law enforcement to abuse GPS tracking and the second being that GPS tracking would impose restrictions on personal freedoms (Kugler and Strahilevitz, 2015. p.251-252).

Importantly, previous research done by Slobogin (2011), Kugler, and Strahilevitz (2015) empirically suggests that the average individual has a high expectation of privacy involving the potentiality of law enforcement monitoring their geographical locations via electronic means. The studies also demonstrate, in contrast of the suspicions of Justice Alito in the *Jones* case, that the duration of GPS tracking is of little statistical significance; tracking for 24 hours is just as intrusive as tracking for a month for the average individual. Most individuals who have a high expectation of privacy regarding GPS tracking cite the potential for abuse and the infringement on personal freedoms. At the same time, individuals who reported a low expectation of privacy often cited the third-party doctrine as the driving rationale behind their expectations.

Importance of Student Perceptions in Research

College students have frequently been the subject of research in the social sciences, particularly in studies of perception, opinion, and expectation. College students offer a convenience sample that allows for mass data to be collected quickly (Peterson and Merunka, 2011, pp.1035-1037). In correlative studies, researchers have observed a

homogeneity in perception responses between society at large and college students (Ok, Shanklin & Back, 2008, pp.5-6).

College students have also been frequent subjects in criminal justice studies. In the field of criminal justice, most subjects are involved as active subjects as respondents to survey methodologies (Payne and Chappell, 2008, pp. 176). Researchers have also frequently used criminal justice students to study perceptions toward different criminological and legal issues (pp. 180). These studies typically serve as convenient opinion polls that gauge topics such as privacy and security (Lawler and Molluzzo, 2009), alternative sentencing methodologies (Payne and Gainey, 1999), and communication between police and civilians (Johnson, 2004).

College students are also particularly relevant in the conversation concerning cell site location tracking and technology based issues (Payne and Chappell, 2008, pp. 185). A recent survey conducted by the Pew Research Center found, in a survey concerning cell phone ownership, that 100% of respondents between the ages of 18-29 owned a cell phone, 94% of which owned a smart-phone. The study also found that college students and college graduates were found to be the most likely education demographic to own a cellular phone (Mobile Cell Phone Usage Fact Sheet, 2018). Furthermore, individuals between the ages of 18-22 are the most likely age group to be involved in crime and criminal activity according to the age-crime curve measurement (Payne and Chappell, 2008, pp.184).

Overall, college students are a worthwhile target population due to their convenience and history of use as respondents. In the case of CSLI tracking, college students are of particular interest because they are the demographic that displays the

highest degree of cell phone ownership and usage. They are also the demographic which disproportionately commits crime, making them likely candidates for the employ of CSLI tracking.

CHAPTER III

METHODOLOGY

Hypothesis

The following are the hypotheses examined in this study.

1. Males will have a higher privacy expectation than females.
2. Individuals of minority races will have a lower expectation of privacy.
3. The older the age of the respondent, the higher the privacy expectation.

Administering the Survey

A survey was utilized to gauge the relationship between the dependent variable of privacy score and the independent variables of gender, race, age, and major. This survey was administered to a total of 1320 students at Middle Tennessee State University across three waves and yielded a combined response rate of 98.8%. This survey was designed to effectively assess the expectation of privacy of respondents in relation to technology driven observation methods. Professors at Middle Tennessee State University agreed to assist in administering the survey by passing the survey out among their students and collecting the results. The results were then collected and brought to the Criminal Justice Department for scoring and coding into the Statistical Package for Social Sciences (SPSS) software.

Respondent Demographics

Survey respondents provided personal and educational information on Section I, questions 1-8 of the survey. Table 1 indicates the mean age of respondents was found to be 21.33 years.

Table 1. Average Age of Respondent

		Privacy	Respondent's age in years
N	Valid	1276	1314
	Missing	44	6
Mean		47.59	21.33
Median		48.00	20.00
Mode		47	20
Std. Deviation		8.133	4.132
Minimum		16	17
Maximum		72	63

Table 2 measured the frequency of respondent's educational classification by year of college. This classification was divided into freshman (19.6%), sophomore (22.9%), junior (31.6%), and senior (25.9%).

Table 2. Respondent's Classification in College

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	1	.1	.1	.1
	Freshman	257	19.5	19.6	19.7
	Sophomore	300	22.7	22.9	42.5
	Junior	414	31.4	31.6	74.1
	Senior	340	25.8	25.9	100.0
	Total	1312	99.4	100.0	
Missing	999	3	.2		
	System	5	.4		
	Total	8	.6		
Total		1320	100.0		

Table 3. Gender of Respondent

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	735	55.7	55.8	55.8
	Male	582	44.1	44.2	100.0
	Total	1317	99.8	100.0	
Missing	System	3	.2		
Total		1320	100.0		

Table 3 measured the gender of the respondent. The results indicated that 55.8% of respondents were female while 44.1% of respondents were male.

Table 4. Race of Respondent

		Frequency	Percent	Valid Percent
Valid	White/Caucasian	795	60.2	60.6
	Black/African American	370	28.0	28.2
	Latino/Hispanic	63	4.8	4.8
	Asian	32	2.4	2.4
	Other	52	3.9	4.0
	Total	1312	99.4	100.0
Missing	System	4	.3	
	Total	8	.6	
Total		1320	100.0	

Table 4 measures the frequency of race among respondents. The participants responded as White/Caucasian (60.6%), Black/African American (28.2%), Latino/Hispanic (4.8%), Asian (2.4%), Other (3.9%).

Table 5 measures frequency by college major. Overall, the study represented respondents from over fifty college majors. A supermajority of these respondents identified as being criminal justice majors (65.2%) while 34.8% stated a major other than

criminal justice. A significant portion of the respondents did not answer this question however (39.8%).

Table 5. Is Respondent CJ Major?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	277	21.0	34.8	34.8
	yes	518	39.2	65.2	100.0
	Total	795	60.2	100.0	
Missing		525	39.8		
Total		1320	100.0		

The respondents also answered questions of their cell phone usage and whether the respondent's cell phone was a smart phone or not. As seen in Table 6, 99.3% of respondents indicated that they utilize their cell phone on a regular basis. Of these cell phone users, 94.9% stated that their cellular device was a smart phone and had connection to the internet (Table 7).

Table 6. Do You Regularly Use a Cell Phone?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	9	.7	.7	.7
	Yes	1309	99.2	99.3	100.0
	Total	1318	99.8	100.0	
Missing	System	2	.2		
Total		1320	100.0		

Table 7. Is Your Cell Phone a Smartphone?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	58	4.4	4.4	4.4
	Yes	1250	94.7	94.9	99.3
	N/A	9	.7	.7	100.0
	Total	1317	99.8	100.0	
Missing	System	3	.2		
Total		1320	100.0		

Survey Instrument

Section I of the survey was designed to gather demographic and cell phone use frequency data on the respondent. The demographic information gathered included gender, race, age, college major, and college classification. The cellular data inquired the regularity of cell phone usage, whether the respondent's phone was a smart phone, and what type of contract plan the respondent had with their cellular provider. Section II entailed eighteen Likert-scale questions designed to gauge the respondent's expectation of privacy. These questions ranged from 1, for "strongly disagree" to 5, for "Strongly Agree." These questions were calculated into a "privacy score" on a range from 1 to 72 with the higher the numerical score indicating a higher expectation of privacy. Five of these eighteen questions were isolated and were considered "questions of legality" in which the respondent answered questions of legality regarding GPS tracking. Section III of the survey tested the legal knowledge of respondents by asking a series of twelve true or false questions regarding the legality of certain actions the state might perform in the course of a criminal investigation. This survey was derived from a previous study conducted by Dr. Lance Selva, Chairman of the Criminal Justice Department and Dr.

Joshua Harms, Assistant Professor at Middle Tennessee State University. The survey was approved for use by the Institutional Review Board (IRB) on February 6, 2017.

Collection of Data

This study consisted of 1320 respondents who participated in a self-administered survey with thirty-eight questions designed to gauge their expectation of privacy. Professors in various departments were contacted and asked to assist the research effort by administering the survey to their classes. If a professor agreed, the researcher provided the survey to the professor and the survey was administered during class. Respondents were then asked to provide information in three sections of the survey. Section I allowed the respondents to provide demographic information, section II was used to gauge the respondent's privacy score, and section III was used to determine the respondent's knowledge of existing privacy law. Since the scope of this study does not require existing knowledge of privacy law, section III was excluded from coding and calculation. The data was then taken by the researcher and coded into an excel file which was then processed into SPSS for calculation. Several tests of significance were performed consisting of: *T*-test, ANOVA, and Pearson-*R*.

Sampling

The unit of analysis for this study was individual students at Middle Tennessee State University. These students were aggregated from a wide variety of college majors and age groups. The respondents for this study were gathered from a convenience sample as the respondents are the individuals who were present in class when the survey was administered. The target demographic is students who attend Middle Tennessee State University and are regular users of cellular devices

CHAPTER IV

RESULTS

This study was created with the intention of measuring the normative privacy expectations of students at Middle Tennessee State University. Following the tabulation of the privacy score, the variables of gender, race, age, and college major were selected and examined with statistical tests used to determine the degree to which these variables effect the normative privacy expectations of respondents.

Gender and Privacy

To determine the statistical significance of gender and its effect on privacy, a t-test was utilized. As seen in Table 8-9, the significance value was found to be .000 with an average privacy score difference of 1.83 numerically. The data indicates that, on average, males tended to have a privacy score that was an average of 1.83 points higher than females. This data confirms the research hypothesis.

Table 8. Privacy by Gender

	Gender of respondent	N	Mean	Std. Deviation	Std. Error Mean
Privacy	Male	561	48.62	8.401	.355
	Female	713	46.79	7.820	.293

Table 9. Independent Samples and Significance

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Privacy	Equal variances assumed	2.950	.086	4.016	1272	.000	1.831	.456	.937	2.726
	Equal variances not assumed			3.982	1159.815	.000	1.831	.460	.929	2.734

Race and Privacy

An ANOVA test was used to determine the average difference of privacy score among different races and the significance of these differences. The results indicated that there are statistically significant results and notable differences between races. Table 10 indicates the average privacy scores by race and Table 11 indicates the results of the ANOVA significance test. African Americans held the highest average expectation of privacy at an average of 48.44 out of 72. Asians held the lowest average expectation of privacy at an average of 43.78 on the 72-point scale. The statistical significance of these results is 0.020, demonstrating a statistically significant test. The hypothesis stated that members of minority races would have a lower expectation of privacy than members of majority races. African Americans were shown to have the highest expectation of privacy

of the races tested. Therefore, the null hypothesis is accepted and the research hypothesis rejected.

Table 10. Privacy by Race

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
White/caucasian	777	47.46	8.548	.307	46.86	48.06	16	70
Black/African American	349	48.44	7.328	.392	47.67	49.21	19	72
Latino/Hispanic	61	47.26	7.998	1.024	45.21	49.31	25	66
Asian	32	43.78	6.226	1.101	41.54	46.03	29	61
Other	50	46.76	7.153	1.012	44.73	48.79	32	60
Total	1269	47.60	8.125	.228	47.15	48.05	16	72

Table 11. Privacy by Race, ANOVA Test

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	771.229	4	192.807	2.939	.020
Within Groups	82929.411	1264	65.609		
Total	83700.640	1268			

Age and Privacy

A Pearson-*R* correlation was used to determine the correlation of age and privacy as well as statistical significance. The calculations found a significance of .000, indicating that the results are statistically significant. The Pearson-*R* was measured at .115 indicating a weak positive correlation between age and a respondent's expectation of

privacy. The hypothesis stated that as a respondent's age increased, the privacy score would also increase. This research hypothesis was found to be valid though the correlation is considered weak. The research hypothesis is accepted. Table 12 demonstrates the results of the Pearson-*R* calculation.

Table 12. Privacy by Age of Respondent; Pearson-R Correlation

		Respondent's age in years	Privacy
Respondent's age in years	Pearson Correlation	1	.115**
	Sig. (2-tailed)		.000
	N	1314	1271
Privacy	Pearson Correlation	.115**	1
	Sig. (2-tailed)	.000	
	N	1271	1276

**. Correlation is significant at the 0.01 level (2-tailed).

College Major and Privacy

To determine statistical significance and numerical variation in the comparison of respondent's college major and privacy, a *T*-Test was utilized. The statistical significance of the test was found to be 0.010, indicating that the results are statistically significant. Analysis of the data determined that that respondents who indicated they were criminal justice majors had an expectation of privacy that was 1.585 points higher on the privacy scale. The average criminal justice major held a privacy score of 48.44 while non-criminal justice majors held a privacy score of 46.85. Table 13 demonstrates the numerical differences of this test. A *t*-test was conducted and yielded a significance value of .001. The research hypothesis of criminal justice majors having a higher expectation of privacy than non-criminal justice majors is affirmed. The null hypothesis is rejected.

Table 13. Privacy by College Major

	Is respondent CJ major?	N	Mean	Std. Deviation	Std. Error Mean
Privacy	yes	503	48.44	8.142	.363
	no	265	46.85	8.109	.498

General Privacy Score

Overall, the mean privacy score among all respondents was found to be 47.59 on the 72-point scale. Respondents consistently demonstrated a high expectation of privacy with the lowest privacy expectation being Asian respondents with a collective average of 43.78. Even this score is substantially higher than the median of the privacy scale (36). Respondents tended to have strong privacy expectations across all waves, across all demographics, and across all variables. The hypothesis is affirmed and the null hypothesis rejected. Table 14 shows the average privacy score among all waves and Table 15 shows the results of an ANOVA test for significance. The ANOVA test indicated a significance value of 0.036, indicating that the results are statistically significant.

Table 14. Average Privacy Score by Wave

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
2012	466	48.32	8.160	.378	47.58	49.06	16	70
2015	452	46.95	8.069	.380	46.21	47.70	22	72
2017	358	47.45	8.125	.429	46.61	48.30	23	66
Total	1276	47.59	8.133	.228	47.15	48.04	16	72

Table 15. ANOVA Test for Significance

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	438.012	2	219.006	3.323	.036
Within Groups	83894.075	1273	65.903		
Total	84332.088	1275			

Isolating Questions of Legality

The researcher specifically isolated questions that dealt with the respondent's perceptions of the legality of law enforcement actions and the legal control mechanism of these actions. Chief among these questions was the respondent's opinion on whether a warrant should be the controlling mechanism of action for CSLI related tracking. Respondents overwhelmingly responded with strong privacy expectations. To the question of whether a warrant should be the controlling legal standard, 85.2% of respondents either agreed or strongly agreed that a warrant from a judge should be the controlling standard in acquiring cell phone data. A super majority of respondents, 81.3%, believed cell phone data should only be acquired once probable cause had been established. Table 16 shows these questions and the corresponding answers on the Likert Scale.

Table 16. Legality Questions

Item	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
The police should only be able to access my cell phone call data by getting a search warrant from a judge.	1.7	4.1	9.0	37.5	47.7
The police should only be able to access my cell phone call data by showing the data is related to an on-going criminal investigation.	2.5	3.4	10.1	43.6	40.4
The police should only be able to access my cell phone call data by showing probable cause to a judge that I am involved in criminal activity.	2.2	6.9	9.6	44.4	36.9
The Fourth Amendment (illegal searches and seizures) should be interpreted to provide citizens with strong privacy protections.	.4	3.4	16.3	48.8	31.0
The Fourth Amendment should be interpreted to allow police unrestricted freedom in uncovering criminal activity.	22.2	35.8	25.0	14.6	2.4

CHAPTER V

DISCUSSION AND CONCLUSION

Discussion

The data from this study yielded important considerations for the privacy debate surrounding CSLI tracking. Of the four hypotheses presented in this study, three were accepted and one was rejected with the null hypothesis accepted. The variables of sex, race, age, and college major were all found to have statistically significant results on the privacy expectations of respondents. Overall, men tended to have higher privacy expectations than women; African Americans tended to have higher privacy expectations than members of other races; older respondents tended to have higher privacy expectations than younger respondents; and respondents who were majoring in criminal justice tended to have a higher expectation of privacy than other majors.

Perhaps what is most interesting however, is the actual deviation of privacy scores tended to be very marginal across all variables. This study echoes the conclusions of the studies done by Slobogin, Kugler, and Strahilevitz. Respondents of all demographics held higher than median expectations of privacy. This suggests that, despite small differences, the average respondent held a significantly strong expectation of privacy despite demographic differences.

In the consideration of the second prong of the *Katz* test, this study provides a successful point of reference for a quantitative examination of the average college student's expectation of privacy. This study also provides an answer as to the perception of citizens regarding CSLI tracking. In this study, it was clear that respondents held high expectations of privacy regarding GPS tracking and the interception of cellular data.

When questioning the perception of the current legal status of CSLI tracking, which does not currently require a warrant, a super majority of respondents indicated that a warrant should be the controlling legal mechanism regarding CSLI tracking. This places the current legal status of CSLI tracking at odds with the perception of respondents in this study.

Limitations of the Study

This study's primary limitation is the lack of a nationally weighted sample. While this study provides an accurate account of the average privacy expectation the average college student, it fails to provide an account of the privacy expectation of the average American. However, based on the results of the Kugler and Strahilevitz studies, which were nationally weighted, the conclusions seem applicable in both scenarios. Another limitation is that the study was a convenience sample of students at Middle Tennessee State University. For a question such as privacy expectation, geography could be hypothesized to play a crucial role and thus having a nationally weighted sample is of paramount importance.

Future Research

It is clear that a greater degree of research needs to be performed before the true societal expectation of privacy can be established. Future research should be nationally weighted with a focus on examining longitudinal trends in privacy expectation. This would allow for researchers to examine societal factors that influence privacy expectations and may yield important insights for the jurisprudence of American Courts.

Conclusion

CSLI tracking and cell data monitoring remains a vital topic of interest and a hotly contested legal battleground. The government holds the position that these cellular emissions are not private and therefor can be captured without a warrant requirement. In the debate of this legal issue, it was recognized that a gap in knowledge existed concerning what privacy expectations American citizens have regarding their location and cellular data. Several studies were conducted, each generally concluding that American's tended to hold high expectations of privacy concerning these issues. This study mirrors those findings. Respondents in this study averaged a consistently high privacy expectation across all demographics and across all questions. Relevant to this debate, 85.2% of respondents in this study disagreed with the current controlling legal standards concerning CSLI tracking and favored a warrant requirement for GPS and cellular data information. While the state of CSLI tracking remains contested and unclear, the results of this study clearly favor stronger privacy rights and more stringent regulation of the governments utilization of cellular data capture.

REFERENCES

Periodicals

Bennardo, C. (2017). The fourth amendment, CSLI tracking, and the mosaic theory. *Fordham Law Review, 85*(5).

Burten, C. (2012). Unwarranted! Privacy in a technological age: the fourth amendment difficulty in protecting against warrantless GPS tracking and the substantive due process and first amendment boost. *Outhern California Interdisciplinary Law Journal, 21*(2), 371-375.

Chamberlain, P. (2004). Court ordered disclosure of historical cell site location information: the argument for a probable cause standard. *Washington and Lee Law Review*, *66*, 1754-1791.

Colb, S. F. (2004). A world without privacy: why property does not define the limits of the right against unreasonable searches and seizures. *Michigan Law Review*, *102*(5), 889-903.

Curtiss, W. (2011). Triggering a closer review: direct acquisition of cell site location tracking information and the argument for consistency across statutory regimes. *J.L. & Soc. Problems, 45*.

Dennis, E. (2011). A mosaic shield: Maynard, the fourth amendment, and privacy rights in the digital age. *Cardozo Law Review*, *33*, 737-771.

Donohue, L. K. (2017). The fourth amendment in a digital world. *Georgetown University Law Center*.

Elgart, C. (2016). The road from Jones: the requirement of reasonableness for a GPS search of a vehicle. *Georgetown University Law Center*.

Ford, V. (2011). Mosaic theory and the fourth amendment: how Jones can save privacy rights in the digital age. *American University Journal of Gender, Social Policy & the Law*, *19*, 1351-1372.

Freiwald, S. (2011). Cell phone location data and the fourth amendment: a question of law, not fact. *Maryland Law Review, 70*, 677-749.

Harkins, S. (2011). CSLI disclosure: why probably cause is necessary to protect what's left of the fourth amendment. *Washington and Lee Law Review*, *68*, 1875-1923.

Hutchins, R. (2007). Tied up in Knotts? GPS technology and the fourth amendment. *U.C.L.A. Law Review*, *55*, 473-497.

Johnson, R. R. (2004) Citizen expectations of police traffic stop behavior. *Policing: An International Journal of Police Strategies and Management*, *27*(4), 487-497.

Kugler, M. B., & Strahilevitz, L. J. (2016). Actual expectations of privacy, fourth amendment doctrine, and the mosaic theory. *The Supreme Court Review, 2015*(1), 205-263.

Kerr, O. S. (2009). Do we need a new fourth amendment? *Michigan Law Review, 107*(6).

Kerr, O. S. (2012). The mosaic theory of the fourth amendment. *Michigan Law Review, 110*.

Lawler, J., & Molluzzo, J. (2010). A study of the perceptions of students on privacy and security on social networking sites (SNS) on the internet. *Journal of Information Systems Applied Research, 3*(12), 3-18.

Lichblau, E. (2012, July 12). Cell carriers called on more in surveillance. *New York Times*

Madden, M., & Rainie, L. (2015, May 20). Americans' attitudes about privacy, security and surveillance. Retrieved from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Mobile cell phone usage fact sheet. (2018, February 05). Retrieved from http://www.pewinternet.org/fact-sheet/mobile/

M. R. H. (1985). Tying privacy in Knotts: beeper monitoring and collective fourth amendment rights. *Virginia Law Review, 71*(2), 297.

McLaughlin, K. (2007). The fourth amendment and cell phone location tracking: where are we? *Hastings Communications and Entertainment Law Journal, 29*.

Ok, C., Shanklin, C. W., & Back, K. (2008). Generalizing survey results from student samples: implications from service recovery research. *Journal of Quality Assurance in Hospitality & Tourism, 8*(4), 1-23.

Ostrander, B. M. (2011). Mosaic theory and fourth amendment law. *Notre Dame Law Review, 86*(4), 1759-1795.

Payne, B. K., & Chappell, A. (2008). Using student samples in criminological research. *Journal of Criminal Justice Education, 19*(2), 175-192.

Payne, B. K. & Gainey, R. R. (2005). Attitudes toward electronic monitoring among monitored offenders and criminal justice students. *Journal of Offender Rehabilitation*, *29*, 195-208.

Peterson, R. A., & Merunka, D. R. (2014). Convenience samples of college students and research reproducibility. *Journal of Business Research, 67*(5), 1035-1041.

Selva, L. H., Shulman, W. L., & Rumsey, R. B. (2016). Rise of the mosaic theory: implications for cell site location tracking by law enforcement. *John Marshall Journal of Information Technology and Privacy Law, 32*(4).

Simmons, R. (2002). From Katz to Kyllo: a blueprint for adapting the fourth amendment to twenty-first century technologies. *Hastings Law Journal*, *53*, 1303-1757.

Slobogin, C. (2011). *Privacy at risk: the new government surveillance and the fourth amendment*. Chicago: University of Chicago Press.

Slobogin, C., & Schumacher, J. E. (1993). Reasonable expectations of privacy and autonomy in fourth amendment cases: an empirical look at "understandings recognized and permitted by society". *Duke Law Journal, 42*(4), 727.

Wallentine, K. (2011). Cell site location evidence: a new frontier in cyber-investigation. *AELE Monthly Law Journal, 401*, 401-415.

Walsh, C. (2012). Surveillance technology and the loss of something a lot like privacy: an examination of the "mosaic theory" and the limits of the fourth amendment. *St. Thomas Law Review, 24*(169).

Legal Cases and Constitutional Provisions

Karo v United States, 468 U.S. 705 (1984)

Katz v United States, 389 U.S. 347 (1967)

Kyllo v United States, 533 U.S. 27 (2001)

Smith v Maryland, 442 U.S. 735 (1979)

United States v Carpenter, 819 F.3d 880 (2017)

United States v Graham, 442 U.S. 735 (2016)

United States v Jones, 132 S. Ct. 945 (2012)

United States v Knotts, 460 U.S. 276 (1983)

United States v Maynard, 615 F.3d 544 (2010)

United States v Miller, 307 U.S. 174 (1976)

Washington v Jackson, 390 U.S. 570 (2003)

Chimel v California, 395 U.S. 752 (1969)

Riley v California, 573 U.S. (2014)

APPENDIX

APPENDIX A: IRB APPROVAL

IRB
INSTITUTIONAL REVIEW BOARD
Office of Research Compliance,
010A Sam Ingram Building,
2269 Middle Tennessee Blvd
Murfreesboro, TN 37129

IRBN001 - EXPEDITED PROTOCOL APPROVAL NOTICE

Friday, February 03, 2017

Investigator(s): James Horton (Student PI), Joshua Harms (FA) Investigator(s') Email(s): jeh62@mtmail.mtsu.edu; joshua.harms@mtsu.edu Department: Criminal Justice Administration

Study Title: Law Enforcemet and Cell Phone Providers: Legal Standards of Privacy
Protocol ID: **17-2135**

Dear Investigator(s),

The above identified research proposal has been reviewed by the MTSU Institutional Review Board (IRB) through the **EXPEDITED** mechanism under 45 CFR 46.110 and 21 CFR 56.110 within the category *(7) Research on individual or group characteristics or behavior* A summary of the IRB action and other particulars in regard to this protocol application is tabulated as shown below:

IRB Action	APPROVED for one year from the date of this notification	
Date of expiration	**2/28/2018**	
Participant Size	600 (SIX HUNDRED)	
Participant Pool	MTSU Students	
Exceptions	Collecting any identifying information from participants is permitted.	
Restrictions	**1. Mandatory signed informed consent** **2. 18 years of age or older**	
Comments	NONE	
Amendments	**Date** N/A	**Post-approval Amendments** NONE

This protocol can be continued for up to THREE years (**2/29/2020**) by obtaining a continuation approval prior to **2/28/2018**. Refer to the following schedule to plan your annual project reports and be aware that

you may not receive a separate reminder to complete your continuing reviews. Failure in obtaining an approval for continuation will automatically result in cancellation of this protocol. Moreover, the completion of this study MUST be notified to the Office of Compliance by filing a final report in order to close-out the protocol.

Continuing Review Schedule:

Reporting Period	Requisition Deadline	IRB Comments
First year report	1/31/2018	INCOMPLETE
Second year report	1/31/2019	INCOMPLETE
Final report	1/31/2020	INCOMPLETE

The investigator(s) indicated in this notification should read and abide by all of the post-approval conditions imposed with this approval. Refer to the post-approval guidelines posted in the MTSU IRB's website. Any unanticipated harms to participants or adverse events must be reported to the Office of Compliance at (615) 494-8918 within 48 hours of the incident. Amendments to this protocol must be approved by the IRB. Inclusion of new researchers must also be approved by the Office of Compliance before they begin to work on the project.

All of the research-related records, which include signed consent forms, investigator information and other documents related to the study, must be retained by the PI or the faculty advisor (if the PI is a student) at the secure location mentioned in the protocol application. The data storage must be maintained for at least three (3) years after study completion. Subsequently, the researcher may destroy the data in a manner that maintains confidentiality and anonymity. IRB reserves the right to modify, change or cancel the terms of this letter without prior notice. Be advised that IRB also reserves the right to inspect or audit your records if needed.

Sincerely,

Institutional Review Board
Middle Tennessee State University