Does the Supreme Court Know What's Best For Us?

Potential Mediators of Public Support for

Three Surveillance Techniques

by

Denise Baker

A Thesis Presented in Partial Fulfillment
of the Requirements for the Degree
Master of Science

Approved August 2012 by the
Graduate Supervisory Committee:

Nicholas Schweitzer, Chair
Evan Risko
Matt Newman

ARIZONA STATE UNIVERSITY

December 2012

ABSTRACT

Very little experimental work has been done to investigate the psychological underpinnings of perceptions of privacy. This issue is especially pressing with the advent of powerful and inexpensive technologies that allow access to all but our most private thoughts -and these too are at risk (Farah, Smith, Gawuga, Lindsell, &Foster;, 2009). Recently the Supreme Court ruled that the use of a global positioning system (GPS) device to covertly follow a criminal suspect, without first obtaining a search warrant, is a violation of a suspect's fourth amendment right to protection from unlawful search and seizure (United States v. Jones, 2012). However, the Court has also ruled in the past that a law enforcement officer can covertly follow a suspect's vehicle and collect the same information without a search warrant and this is not considered a violation of the suspect's rights (Katz v. United States). In the case of GPS surveillance the Supreme Court Justices did not agree on whether the GPS device constituted a trespassing violation because it was placed on the suspect's vehicle (the majority) or if it violated a person's reasonable expectation of privacy. This incongruence is an example of how the absence of a clear and predictable model of privacy makes it difficult for even the country's highest moral authority to articulate when and why privacy has been violated. This research investigated whether public perceptions of support for the use of each surveillance technique also vary across different monitoring types that collect the same information and whether these differences are mediated by similar factors as argued by the Supreme Court. Results suggest that under some circumstances participants do demonstrate

differential support and this is mediated by a general privacy concern. However, under other circumstances differential support is the result of an interaction between the type of monitoring and its cost to employ -not simply type; this differential support was mediated by both perceived violations of private-space and general privacy. Results are discussed in terms of how these findings might contribute to understanding the psychological foundation of perceived privacy violations and how they might inform policy decision.

ACKNOWLEDGMENTS

I would like to thank my husband Thomas, for his blind faith in everything I do, his steadfast encouragement for all that matters to me, and his unbounded witticisms that keep me moving. I would also like to my express my sincere gratitude and appreciation to Dr. Nick Schweitzer for the countless hours he has devoted to this and many other projects I have done. His ardent and unwavering dedication to my success and his inexhaustible intellect are deeply cherished. I would also like to warmly thank Dr. Evan Risko, who's creative and optimistic approach to science is inspiring and whose help and guidance are invaluable. Finally, I would like to thank Dr. Matt Newman, not only for being on my committee, but also for waiting patiently and being so flexible.

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

Figure Page

Chapter 1

INTRODUCTION

There is no clear consensus on what the definition of "privacy" should be, though many legal and philosophical scholars have attempted to define it (Parent, 1983; Parker, 1973; Otterburg, 2004; Suslak, 2011; Nissenbaum, 1998). The absence of a clear definition is particularly problematic in the United States, not only because this leaves our legal system responsible for resolving privacy protection issues without knowing specifically what should be considered private, but also because our penchants for newer, better, and cheaper forms of information technologies almost inevitably result in new ways, whether intentionally or not, of accessing information that, prior to, was intuitively considered "private." As each new perceived threat to privacy is brought before the legal system, law makers must redefine what information should be legally protected and what should be considered public domain -and why it should be so. In terms of moving to a more predictive model of privacy protection, rather than the backward-looking process that exists today, understanding "why" is key in determining "what." Recently, in an attempt to make defining privacy more practical, experimental researchers have begun to attempt to identify the mechanism or mechanisms by which privacy decisions are made (Baker, Schweitzer, Risko, submitted). Being able to recognize what mediates privacy decisions under a variety of circumstances would be invaluable to the legal system in terms of being able to create policies that accurately consider underlying public interests.

Significant privacy issues that arise from the government's use of technology to collect information about its citizens generally arrive at the Supreme Court arguing for protection under the fourth amendment which provides citizens protection against unreasonable search and seizure (Otterburg, 2004; Parker, 1973). It is up to the individual Supreme Court justices to decide what is and is not considered private, and often when these decision are made, even when a unanimous decision in terms of end outcome is reached, they are justified for different reasons (Thrifty-Tel, Inc v. Bezenek, 1996; United States v. Pineda-Moreno, 2010; United States v. Jones, 2012). As technology allows a wider range of information to be monitored by many parties including the government (such as long range video surveillance, genetic information, social media interactions, internet history usage, etc.) each new attempt to use such information to identify illegal activity inevitably becomes scrutinized as a potential privacy violation The changing nature of technology and the short-sighted ways in which privacy is defined make it difficult for existing rulings to be applied across multiple technologies.

One particular example of a technological advance in surveillance that outpaces privacy policies is the unprecedented ability to record and transmit a detailed and persistent stream of information about a person's geographical location, which quickly presented unaddressed legal concerns about threats to privacy (Ackerman, 2012; Nissenbaum, 1998). The extent of these threats was and still is not universally agreed upon (Otterburg, 2004; Totenberg, 2011; Friedman, 2012), resulting in inconsistent policy decisions about the use of this

technology (United States v. Jones, 2012; United States v Pineda-Moreno, 2010). The constitutionality of using this type of technology, specifically the use of a global positioning system device or receiver (GPS), to covertly track criminal suspects has been debated in both State and Federal courts and by legal scholars and philosophers (United States v. Jones, 2012; United States v Pineda-Moreno, 2010; United States v. Robinson, 2011; Suslak, 2011; Otterburg, 2004; Friedman, 2012, Shah, 2009). The arguments fall not on whether law enforcement officers (LEO's) can use GPS technology in general, but specifically whether they can do so without first obtaining a search warrant. The argument has been essentially put to rest with the Supreme Court's 2012 decision (United States v. Jones, 2012) declaring that a GPS device may no longer be covertly placed on a suspect's vehicle without first obtaining a valid search warrant, citing that this would be a violation of the suspect's fourth amendment rights. The Supreme Court justices reached a unanimous decision in this case, however they were split five to four as to why the decision should have been made and argued two different precedents were argued to each be the more relevant that the other in terms of which one to base the ruling. When stepping back to consider relevant aspects of the nature of the information being protected (i.e details information about a suspect's vehicle location) it presents as an interesting example of the ambiguity of privacy policies, for if this same type of covert surveillance is conducted without a search warrant, but carried out by an LEO in an undercover vehicle, no such privacy violation occurs. In other words, a law enforcement officer can surreptitiously follow a suspect's vehicle and record detailed information about the vehicle's

location for any continuous period of time (referred to here as "tailing") without a search warrant, but this same information obtained through the use of a GPS device without a search warrant is unconstitutional. The case of United States v. Jones (2012) demonstrates that in terms of privacy, law makers do not consistently agree on how and why privacy decisions should be made. As the legal system continues to grapple with constructing a framework to guide the legal use of covert surveillance with respect to the fourth amendment, little attention has been dedicated to understanding public perceptions of such surveillance techniques or the mechanisms that guide these decisions as a means to understanding the nature of privacy itself. To that end, this research will not attempt to directly define privacy, but will instead 1) investigate if the public also perceives an intuitive difference between types of monitoring that collect similar information, and 2) investigate if those perceptions are mediated by factors that echo the arguments presented in United States v. Jones (2012).

Law Enforcement Surveillance

Law enforcement agencies often rely on covert surveillance to collect information about a criminal suspect in order to gather evidence for an investigation (Marx, 1989; Shah, 2009). This type of surveillance can be accomplished a number of ways that range from mundane to highly complex; from collecting documents, to following a shoplifter through a store, to setting up intricate and lengthy stake-outs. In some cases, monitoring the location of a suspect's vehicle can be a fundamental part of an investigation. Methods employed to conduct this type of surveillance can consist of using undercover

LEO's to follow a suspect's vehicle in unmarked cars while keeping the suspect vehicle in view, or by using a radio frequency tracking device (RF tracker) placed surreptitiously in a suspect's possession to track the suspect vehicle from a short distance without being in view of the vehicle (Marx, 1989; Shah, 2009, United States v. Knotts). In both cases the agency can record detailed information about the vehicle's location at all times during the surveillance period and, so long as the vehicle remains in public view, these agencies can utilize either method without first obtaining a search warrant (United States v. Karo). Since the early 2000's however, law enforcement agencies have had increased access to GPS tracking devices as an alternate form of covert surveillance. Originally designed for military navigation in the late 70's, the global position system as a whole became available for public use in 1996 when President Clinton declared the network to be reclassified as a "dual-use," program (McLeod, 2008) opening the GPS market to civilians. Since 1996, GPS devices have steadily declined in price and increased in accuracy, making them an inexpensive and effective technology freely available to both governmental and private entities (Economist, 2007; Shah, 2009). Law enforcement can attach a GPS device covertly to the suspect's vehicle and gather detailed information about the suspect's vehicle location as with previously mentioned form of surveillance; however an LEO can track this information from a police station or other remote location rather than necessarily maintaining close proximity to the suspect vehicle. The GPS device is appealing to law enforcement agencies because it enhances officer safety by removing LEO's from the street, it is effectively inescapable unless there is a malfunction or

the device is discovered and removed, and it is relatively inexpensive (Eckholm, 2012). In addition to GPS devices, some law enforcement agencies are piloting a form of surveillance that would provide both vehicle location data and visual data through the use of low flying, unmanned aircraft (often referred to as aerial drones) equipped with high resolution cameras and GPS technology (BBC News, 2012). While RF trackers, tailing, and GPS devices can collect similar information, they are not created equal in terms of their constitutionality; the admissibility of warrantless drone surveillance has yet to be argued at the Supreme Court level. The legal precedents used in the Supreme Court's decision to differentiate GPS monitoring from the other forms mentioned here is distinctly divided among the nine Supreme Court Justices and it is this difference in opinion that is uniquely interesting in terms of perceptions of privacy violations.

Divided Legal Opinion

In January, 2012, the Supreme Court of the United States unanimously concluded that attaching a GPS device to a suspect's vehicle to monitor the vehicles location, in absence of a search warrant, violates a suspect's Fourth Amendment rights (United States v. Jones). The majority opinion delivered by Justice Scalia, was that the placement of the device was unconstitutional on the grounds that the attachment of the device to the vehicle constituted trespassing. However, four Justices argued that the information the GPS collected constituted a search and that the search ultimately violated a more relevant precedent of the suspect's reasonable expectation of privacy. Justice Sotomayor explained that while the trespassing did take place, this alone did not sufficiently address

reasonable expectations of privacy, noting that a GPS device would gather and record detailed information not necessarily related to the case and would ultimately provide information about the suspect's self-identity. Sotomayor also noted that GPS technology may pose a unique potential for abuse because it is "relatively easy and cheap" (United States v. Jones), abuse that would threaten the goal of the Fourth Amendment to protect citizens from pervasive government surveillance. While Scalia addressed a more concrete basis that can be compared conventionally to police tailing or drone use, Sotomayor points to a subjective rationale that is less clear in terms of how it differentiates between say police tailing or RF tracking (Otterberg, 2004). Whether the public perceives GPS tracking or similar emerging technologies (such as drones) as fundamentally different from police tailing, in terms of potential privacy violations, has not been investigated. As such, if a differentiation does exists whether the basis for that perception would be grounded in some sort of private-space violation, such as trespassing, or in something more broadly defined as one's "subjective right to privacy," has also been left unexamined.

Trespass vs Search

An inclusive description of trespassing is any unlawful interference that obstructs the individual or the individual's property (Thrifty-Tel, Inc. v. Bezenek, 1996). This definition could also be conceptualized as an invasion of personal and/or physical space. It seems reasonable to expect that if a particular form of monitoring were classified as trespassing, it would also be an intrusion of the suspect's personal and/or physical space.

A search has been defined in legal terms as occurring when "the government violates a subjective expectation of privacy that society recognizes as reasonable" (Smith v Maryland, 1979; Katz v. United States, 1967). This definition obviously poses a complex problem in terms of measurability, implying that the only honest way to define something as legitimately violating a person's reasonable expectation of privacy is to conduct a survey. In practice, this is not how Fourth Amendment violations of unlawful search are decided, and if it were, it would still offer little insight into what mechanisms those expectation were constructed by. Nonetheless, understanding if it is this subjective expectation of privacy that most concerns the public about surveillance, rather than a private-space violation, will at the very least reinforce the need for researchers to identify the specific mechanisms that can predict when an unlawful search would occur or a violation of one's "reasonable expectation of privacy", an understanding which could then be applied in future cases involving emerging surveillance technologies that will undoubtedly pose similar perceived threats to these expectations of privacy (Bilton, 2012).

Summary

The vast majority of research regarding privacy violation and GPS surveillance has focused on the philosophical and legal aspects of how the technology should be employed by government agencies (Nissenbaum,1998; Culnan & Armstrong, 1999; Parent, 1983; Parker, 1973). Research has not, however, investigated public perceptions of GPS and other forms of covert surveillance in attempt to identify what grounds potential privacy concerns in this

area. Although perceptions of privacy are highly subjective (e.g cultural norms may cause differences), prone to unpredictability (e.g. people may freely share information in one situation, but consider this same information secret in another) and have high variability (e.g. privacy expectation may change over time), this research will investigate, in particular, whether public privacy concerns about covert surveillance echo those of Justice Scalia in terms of a private-space violation or those of Justice Sotomayor in terms of a reasonable expectation of privacy. By comparing support for the use of different modes of surveillance that ostensibly collect similar information, perceived privacy violation and perceived private-space violations can be compared as potential mediators. By manipulating factors surrounding the circumstances of the surveillance such as cost and effectiveness, any changes in subjective privacy concerns can also be identified. This is important because, although policy decisions are sometimes made contrary to public opinion, it is nonetheless valuable to be aware of those perceptions, and the underlying factors that motivate them, to make decision that consider public interest more accurately in the future.

Three forms of monitoring will be used for comparison: An attached monitoring device (e.g. GPS); Law enforcement officers (tailing); and an unattached tracking device (e.g. aerial drone). These three modalities are considered for two primary reasons: To investigate if variations in public support corresponds to variations in Supreme Court's decision and to provide variability in physical location of the tracking devices (i.e. GPS physically touches the suspect vehicle, LEO tailing is not touching the vehicle, but is within normal

human visual field, and a drone is relatively much farther away than both GPS and tailing). In addition, investigating support and privacy perceptions of an emerging technology that has not yet been tested in the Supreme court - such as aerial drones- adds value by potentially providing insight into public perception before a policy decision is made. The first experiment will investigate whether the three forms of monitoring, when conducted without a warrant are differentially supported and whether that differentiation is mediated by perceived violations of private-space (which would implicate concerns about trespassing as articulate by Justice Scalia) and/or perceived as a violation of the suspect's and the participant's privacy (which would implicate concerns about an unlawful search as articulate by Justice Sotomayor). The second experiment will then expand on and refine the first by systematically manipulating characteristics of the tracking technologies that may also impact judgments of support, including relative cost and the effectiveness of the monitoring type. In addition to investigating judgments of support across these manipulations, this second experiment also investigated the effect these manipulations may have on those potential mediators.

Chapter 2

EXPERIMENT 1

The first experiment investigates whether participants differentially support the use of three forms of warrantless tracking techniques. This experiment also investigates if these differentiations are mediated by perceived violation of private-space and/or perceived violation of general privacy. Should a differentiation be mediated only by concerns about private-space violations, we would predict that general privacy concerns would not predict differential support and might infer that the public is most concerned about the trespassing aspect of these surveillance techniques. Conversely, should a differentiation be mediated by concerns about only general privacy violations, we would predict that concerns about violations of private-space would not predict differential support and thus we might infer that the public is most concerned about a violation of one's reasonable expectation of privacy with respect to these surveillance techniques. If both private-space and general privacy violations mediate a differentiation in terms of support for the monitoring type this would indicate that concerns raised by both Justice Scalia and Justice Sotomayor (United States v. Jones, 2012) represent public perceptions in this case. In consideration of this possibility the experiment will also investigate whether perceptions of effectiveness may potentially mediate differential support for the three monitoring types.

Method

Participants. Using Amazon Mechanical Turk (AMT) a demographically diverse sample of US residents age 18 years or older was recruited to participate in an online experiment for modest compensation (Rand, 2012; Burhmester, Kwang, & Gosling, 2011; Paolacci, Chandler, & Ipeirotis, 2010) [1]. Participants gained access to the research through AMT's website, this in turn redirected them to an online-experiment conducted using LimeSurvey which is an open-source on-line survey application hosted through ASU virtual servers. A total of 255 responses were received. Consistent with earlier research using similar materials (Schweitzer, Lovis-McMahon, & Baker, submitted; Schweitzer et al., 2011) participant responses were excluded for completing the experiment in less than 60 seconds, participants were also excluded for excessive missing data, and for failing a two question manipulation check (those who received a zero and those who were unable to answer the question asking them to identify the monitoring type they had just read about were categorized as a fail). The final sample excluded 29 responses or 10.7% of the original sample, leaving a total 226 participants of which 54.6% were females, the mean age was 34, and 49.9% held at least a four-year college degree.

Materials/Procedure. Participants were instructed that they would be reading a short scenario, and that it was important they take the time to

[1] The final screen of the survey directed participants back to MT to claim compensation of $1.00 which was consistent with surveys of similar length available through AMT.

understand it. They were also told that they would be answering a series of questions specific to that scenario.

The scenarios asked participants to imagine that the "Association of Police Chiefs" was considering the use of a particular monitoring type to follow suspects and gather information that could lead to an arrest. Using a between-subjects design, each participant was randomly assigned to a scenario with one of three monitoring types. In the GPS condition the GPS device was described as being covertly placed under a suspect's car. In the aerial Drone condition the Drone was described covertly tracking the suspect from the air. Finally, in the Police tailing condition the officers were described as covertly following the suspect using undercover cars.

After reading the scenario, participants were asked to indicate whether they would support the use of the monitoring technology if it were proposed in their state. In this first experiment support was measured as a dichotomous (yes or no) dependent variable, similar to how citizen would express support in a referendum or election. However, rather than rely on this single measure of the dependent variable of support, participants were subsequently presented with a series of thirteen questions, of which three items asked about other aspects of support. Additional items measured perceptions of personal space violations, general privacy violations of both the suspect and the participant, and effectiveness. Participants provided responses using a 7-point Likert scale ranging from "not at all" to "very" judging the extent to which the participant believed their monitoring type would, for example, "…be a violation of the suspect's

personal space," "…constitute a violation of the suspect's privacy," "help catch/apprehend criminals."(See Appendix B for full list of questions). To ensure participants attended to the materials, the following screen presented a manipulation check asking participants to identify the monitoring type in their scenario and the stated purpose of the proposed monitoring technique. Finally, basic demographic information was also collected and upon completion participants were directed back to AMT to receive their compensation

Results

To test the hypothesis regarding differential support for warrantless tracking modalities, rather than simply using the single dichotomous response to the support questions, a maximum likelihood factor analysis with promax rotation was performed using the additional support items (see Appendix B, items 2-4) to determine if a more robust measure of support could be created. From this analysis one factor emerged explaining 82.5% of the variance therefore the four items were converted into a standardized factor score, which was labeled Support. A one-way, between subjects analysis of variance (ANOVA) compared Support scores between the three monitoring types. A significant difference between monitoring modalities in terms of Support was found, $F(2,220)=6.276$, $p=.002$, $\eta^2=.054$. Tukey's post-hoc tests of the three monitoring types indicated that participants were significantly more supportive of Police than Drones (M=.305, M=-.251, $p=.002$) and were approaching significantly greater support for Police

over GPS (M=.305, M=-.046, p=.066). No significant difference in Support between GPS and Drones was found (p=.387).

To investigate if a private-space violation might mediate the relation between Type and Support a one-way ANCOVA was conducted using the Personal Space item as a covariate. This analysis is a preliminary way to test for potential mediation by partialling out its effects and determining if the interaction becomes non-significant (Fiske, Kenny, & Taylor, 1982). This still yielded a significant result indicating Personal Space is not likely a mediator, $F(2,216)=4.812$, p=.009. To investigate privacy violation as a potential mediator, a maximum likelihood factor analysis with promax rotation of the remaining questions 5, and 7-14 (see Appendix B) was conducted, from which two factors emerged. However, four of the items had communalities below 0.4 suggesting they may not be related to the other items (Costello & Osborne, 2005) and this analysis only explained 65% of the total variance, therefor these four items were excluded and the analysis was repeated with questions 5, 8, 11, 12, and 14 from which two factors emerged (See Table 1 for structure matrix) this time explaining 76.05% of the variance. The first factor included items related to privacy violations and the second included items related to effectiveness so these were converted into standardized factor scores and labeled Privacy and Effectiveness. The two factors were negatively correlated, (-.509) indicating that as perceived privacy violation increases, perceived effectiveness decreases.

Table 1

Structure Matrix for Privacy and Effectiveness

Item	**Factor 1**	**Factor 2**
Will Reduce Crime (11)	-.486	.984
Will Help Catch Criminals (12)	-.459	.848
Will Violate Your Privacy (14)	.943	-.449
Will be Abused (8)	.754	-.548
Will Violate Suspect's Privacy (5)	.801	-.385

A one-way ANCOVA using the Privacy factor score as a covariate yielded a non-significant results, $F(2,202)=1.313$, $p=.271$, indicating this could be a potential mediator. This analysis was repeated using the Effectiveness factor score as the covariate and once again a non-significant result was found, $F(2,202)=2.421$, $p=.091$, indicating it too could be a potential mediator. To further explore the effect of these two factors, a mediation analysis was conducted using PROCESS, which is a statistical tool designed to assess direct and indirect effects in models with multiple mediators (Hayes, 2012; Preacher, Rucker, & Hayes, 2007). To accommodate the categorical variable, Type, two dummy codes were created in order to compare GPS to Police, and Drones to Police with Support as the outcome variable. Results indicated that the difference in Support between GPS and Police was completely mediated by Privacy (Indirect effect on Support for GPS vs. Police through Privacy: ab=.1791, SE_{ab}=.0947, 95%CI:[.0015 <ab<.3730]. Indirect effect on Support for GPS vs. Police through Effectiveness: ab=.1202, SE_{ab}=.0677, 95%CI:[-.0061 <ab<.2499]) (See Figure 1). The more

participants viewed GPS as a privacy violation the less likely they were to support its use. The difference in Support between Drones and Police was completely mediated by both Privacy and Effectiveness (Indirect effect on Support for Police vs. Drones through Privacy: ab=.2982, SE_{ab}=.1037, 95%CI:[.0981 <ab<.5096]. Indirect effect on Support for Police vs. Drones through Effectiveness: ab=.1551, SE_{ab}=.0692, 95%CI:[.0183 <ab<.2997])(See Figure 2). The more participants felt Drone was a privacy violation and the more they felt it was not effective, the less likely they were to support its use.

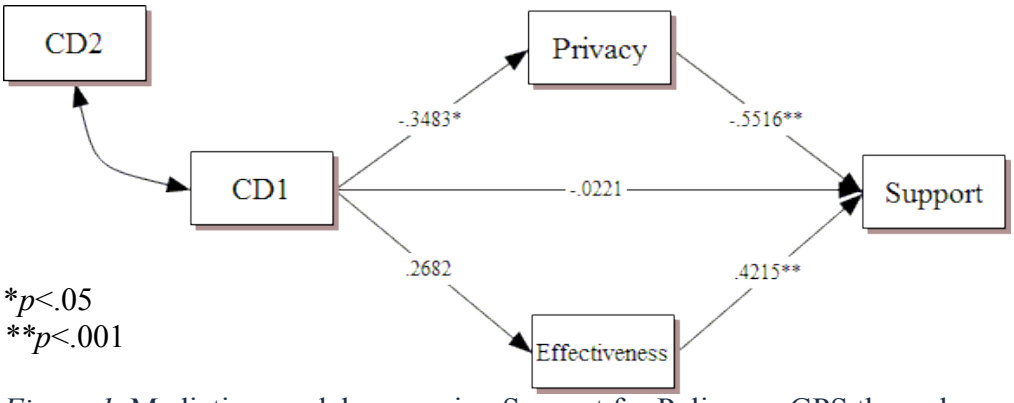
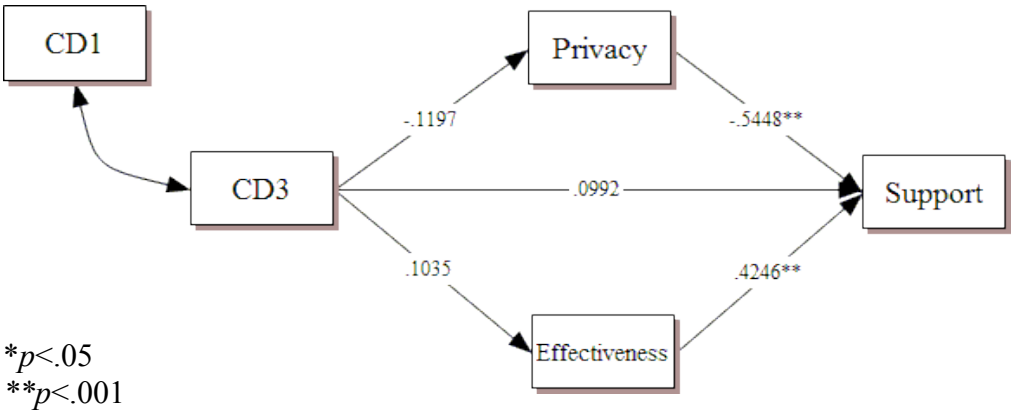


Figure 1. Mediation model comparing Support for Police vs. GPS through Privacy and Effectiveness.



*p<.05
**p<.001

Figure 2. Mediation model comparing Support for Police vs. Drones through Privacy and Effectiveness.

Discussion 1

These results indicate that participants do differentially support these three modes of surveillance and are less supportive of using a GPS device to track suspects than using Police tailing. Further the results indicate that these differences in support are not mediated by perception that monitoring type might violate one's personal space (as might be expected if trespassing were a concern). Instead, it seems that support for one monitoring type over another is mediated by the extent to which a person thinks that it will violate privacy in general, which is more in line with Justice Sotomayor's sentiment that privacy policies concerning certain types of surveillance should be based on protecting a person's reasonable expectation of privacy.

It is important to acknowledge that this experiment was meant to serve as a starting point and did not address some important questions. The second experiment expands on the first by addressing underlying assumptions that might have influenced participants to be more supportive of one form of monitoring compared to another. For example, the terms "GPS" and "Drone" may have negative connotation and/or preexisting expectation of the other capabilities of the technologies (beyond tracking vehicle location) so in experiment two these terms will be replaced with more ambiguous terminology. To investigate if abuse of the technology because of assumptions about low cost influences judgments of Support, the cost of implementing the monitoring type is manipulated in terms of costing more of less than existing surveillance techniques. To determine if

assumptions about effectiveness might influence judgments of support, a criminal suspect's ability to evade the monitoring type is also manipulated. To address whether perceived personal-space violation is a complete measure of private-space violation, an additional item measuring perceived physical-space violation is added.

Chapter 3

EXPERIMENT 2

Using similar vignettes to the previous experiment, one of three forms of warrantless tracking technology (Type) is presented to participants. The cost (Cost) to employ the each monitoring type and the effectiveness (Evade) of each monitoring type are also manipulated. The extent to which the participant would support the use of the monitoring type in their scenario will be used as the primary dependent variable. Potential mediation by private-space violation, privacy violation, and effectiveness will also be examined.

Method

Participants

Again using Amazon Mechanical Turk a demographically diverse sample of US residents, age 18 or older was recruited to participate in an online experiment[2] in exchange for compensation of $1.00. Participants gained access to the research in the same manner as experiment one. A total of 398 responses were received. Because this experiment had two additional screens the cut off time was increased to 120 seconds, and the manipulation check was increased to four questions. A total of 77 response were excluded for failing either the time requirement, for receiving a score of two or less on manipulation check, or for excessive missing data. The final sample excluded 18.6% of the original sample

[2] Participants were instructed not to complete the study if they had participated in a similar study in the past. In addition, by comparing users' IP addresses and finding no duplication between E1 andE2, it was determined that it was unlikely that any participants completed both experiments.

leaving a total 324 participants of which 51.7% were female, the mean age was 31, and 44.9% held at least a four-year college degree.

Materials and Procedure

Using similar vignettes and instruction as in experiment one participants were presented with a scenario about the proposed use of a particular type of monitoring. Once again, three different forms of warrantless tracking technology (Type) were used, however, to avoid potential negative stereotypes the terms "GPS" and "Drone" were replaced by Electronic Tracking Device (Attached Device) and Remote Electronic Tracking (Unattached Device) respectively. These two forms of tracking were still described as covert forms of monitoring a suspect's vehicle location; however, to maintain variability in the physical distance from the suspect and suspect's vehicle, the Attached Device was described as being physically placed on the vehicle and the Unattached Device was described as being remotely located. This experiment also manipulated the cost of implementing the monitoring type (Cost) and a criminal suspect's ability to evade the monitoring type (Evade). Thus, a 3(Type: Electronic Tracking Device, Remote Electronic Tracking, and Full-time police) x 2(Cost: less expensive, more expensive) x2 (Evade: possible, not possible) between-subject design was conducted.

Each participant, after being randomly assigned to one of these twelve conditions, was presented with a scenario informing them the "Association of Police Chiefs" was considering the use of a particular monitoring type to follow suspects and gather information that could lead to an arrest. This was followed by

a statement briefly describing the monitoring type and that information collected would be compared with other police information to identify possible illegal activities. This was followed by a statement that the monitoring type would be more or less costly than current methods available, and this was followed by a separate statement about whether it was possible or not for the suspects to evade the technology. Finally, each scenario concluded with a statement that the monitoring technology would be implemented in such a way that no search warrant would be needed to conduct this particular type of surveillance. A sample scenario and description for each condition is included as Appendix C.

After reading the scenario, participants were asked to indicate whether or not they would support the use of the monitoring technology if their state were to propose its implementation. Although in experiment one this dependent variable was dichotomous, which would correspond to traditional voting procedures, in this experiment a 7-point Likert scale was used to measure participants' relative degree of support (with 1 being "would not support at all" and 7 being "would completely support") to achieve a more precise measure of support. The general support question was followed by a similar set of randomly ordered questions as in experiment one related to effectiveness, privacy, and support (See Appendix B for list). On the next screen participants were presented with a four-item manipulation check to measure whether participants had attended to the information presented in the scenario. Finally, demographic information was collected and participants were directed back to AMT to receive their compensation.

Results

To create the primary dependent variable, a maximum likelihood factor analysis was performed using the same four support questions that were used in experiment one (see Appendix B) from which a single factor emerged, explaining 83.63% of the total variance. The items were converted into a standardized factor score, which was labeled Support. Subsequently, a 3(Type: Attached Device, Unattached Device, and Full-time police) x 2(Cost: less expensive, more expensive) x2 (Evade: possible, not possible) between-subject ANOVA on Support was used to test for main effects and interactions of Type, Cost, and Evade. Interestingly, there were no main effects of Type (p=.137), Cost (p=.779), or Evade (p=.238). There were no significant interactions found between Type and Evade, Evade and Cost, or Evade, Cost, and Type, however there was a marginally significant interaction of Type and Cost. $F(2,309)=2.544$, p=.080, η^2=.016 (see Figure 3).

In order to investigate this potential interaction, simple effects test were conducted to look at Cost within each Type on Support. Within the Attached Device condition, participants showed marginally more Support for the use of the more expensive Attached Device compared to the less expensive Attached Device (p=.109, M=.224, M=.112). In contrast, within the Police condition, participants showed marginally more Support for less expensive Police over more expensive Police (p=.112, M=-.051, M=.230). Within the Unattached Device

condition Support did not significantly differ between the less expensive and more expensive conditions (p=.493).

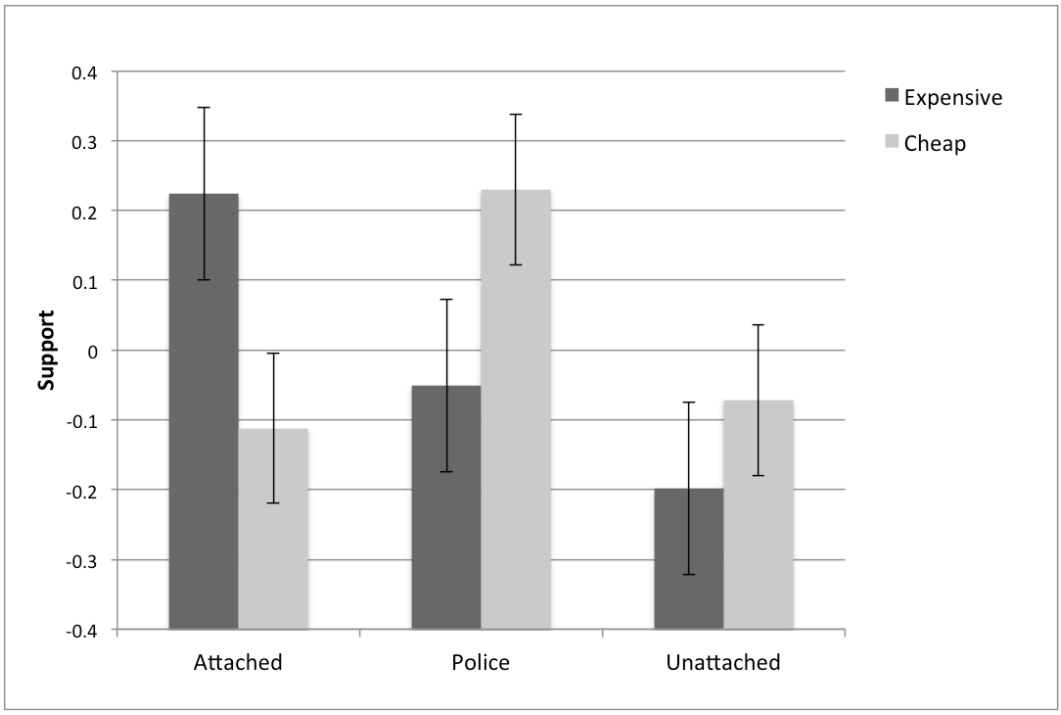


Figure 3. Weak interaction of Type by Cost on Support (p=.08).

To look for a potential explanation for this weak interaction the follow-up questions were examined as potential mediators of the interaction effect. Scores measuring private-space violations were first examined by conducting a set of 3(Type: Attached Device, Unattached Device, and Full-time police) x 2(Cost: less expensive, more expensive) x2 (Evade: possible, not possible) between-subject ANCOVAs, the first using the item measuring physical space violation as a covariate and the second using the item measuring personal space violation as a covariate. The Type x Cost interaction was no longer significant when Physical Space (p=.226) was included as a covariate, indicating potential mediation. The

interaction was also no longer significant when Personal Space (p=.270) was included as covariates, also indicating potential mediation. We continued by examining the item that asked participants if they felt their monitoring type would be used to often. Once again a 3(Type: Attached Device, Unattached Device, and Full-time police) x 2(Cost: less expensive, more expensive) x2 (Evade: possible, not possible) between-subject ANCOVA was conducted with Used to Often as a covariate. In this analysis the interaction between Type and Cost remained weakly significant (p=.093) indicating participant responses on this item was not likely mediating the Type by Cost interaction. Subsequently, as in experiment one, to investigate whether privacy or effectiveness mediated this relationship a maximum likelihood factor analysis with promax rotation was performed using questions 5,7, and 9-14 (see Appendix B), from which two factors emerged. However, three items had communalities below 0.4 and the analysis only explained 53% of the total variance, therefor these three items were excluded and the analysis was repeated with questions 5, 10, 11, 12, and 14. Once again two factors emerged, this time explaining 73.89% of the total variance. The items loaded into factors in a similar fashion as experiment one and were also negatively correlated (-.422). Two standardized factor scores were created and labeled Privacy and Effectiveness. In two subsequent ANCOVA's, the Privacy factor score was entered as a covariate as was the Effectiveness factor score. The weak interaction of Type by Cost remained when Effectiveness was used as a covariate (p=.065),indicating this factor is not likely a mediator, however the

interaction was no longer significant when the Privacy factor was included as covariate (p=.603), implicating it as a potential mediator of this interaction.

Table 2

Structure Matrix for Privacy and Effectiveness

Item	**Factor 1**	**Factor 2**
Will Reduce Crime (11)	-.383	.930
Will Catch Criminals (12)	-.332	.737
Violates Suspect's Privacy (5)	.939	-.386
Violates Your Privacy (14)	.873	-.367
Provides Too Much Info (10)	.800	-.364

Discussion 2

Results from experiment two indicate that differential support for each monitoring technique may be effected when the monitoring type is described in terms that may prevent participants from immediately accessing existing stereotypes. These findings could be significant to decision makers when comparing existing and emerging technology that are functionally similar, but may carry significantly different public perceptions. These results also revealed an interesting interaction between monitoring Type and Cost, specifically when comparing support for the use of an Attached device and Police tailing. Participants were more supportive of the "more expensive" Attached Device than the "less expensive" one, but the opposite was true of using Police tailing (participants were more supportive of "less expensive" Police tailing). This interaction was mediated by perceptions of private-space violation and general

privacy violation which would suggest that, both precedents addressed in United State v Jones, (trespass and reasonable expectation of privacy) mediate public decision of support for this interaction.

Chapter 4

GENERAL DISCUSSION

Experiment one suggest that the public's intuitive decisions about support for the use of GPS devices without a search warrant are congruent with the Supreme Court's ruling in United v. Jones (2012) that covertly tracking a suspect using a GPS device without a search warrant is unlawful. However, in this case the extent to which participants were less supportive of using the GPS device (and more supportive of Police tailing) was mediated by the extent to which the monitoring type was perceived to be a threat to general privacy and was not mediated by perceived threats to private-space. This indicates that, based on their instinctive knowledge of the technology, the public is less supportive of GPS devices for a different reason than that of the majority opinion indicating that GPS tracking is a violation of the Fourth Amendment on the grounds that placement of the device constitutes trespassing (United States v. Jones). While experiment one provides evidence that the public does differentially support monitoring types that purportedly collect similar information, experiment two, which was designed to strip away and control for preconceptions about the technologies, demonstrated that without the extra baggage associated with the terms "GPS" and "Drone" the public may not necessarily exercise differential support for these monitoring types.

To understand these findings it is necessary to look more closely at the design and results of each experiment. In the first experiment participants were

ask to make judgments about technologies that they have most likely seen or heard about in a variety of media outlets, as such the terms GPS and Drone arguably come to the table with preexisting connotations in terms of their use by law enforcement. For example drones have traditionally been used by the military in combat zones which could evoke a negative stereotype, and a GPS receiver is so regularly included as a component in other more sophisticated devices (such as cell phones) it may be difficult for participants to disassociate all of these other functions from simple location tracking, potential evoking the intuition that a GPS device may gather too much information (Maass & Rajagopalan, 2012). Nonetheless, it is important to know if and how these baseline or intuitive decision influence support and perceived privacy violations because, in the "real world", this is generally what public participation in policy decision will be guided by. Experiment one examined what mediates these intuitive measures of support, which, again are important to acknowledge and investigate, but experiment two demonstrates that these mechanisms are not necessarily the same when these preconceptions are removed.

In the first experiment we find that participants' differential support for the three monitoring types was mediated by the extent to which the monitoring type was perceived to be a threat to overall privacy. However, these perceptions of potential privacy violations could be influence by a number of pre-existing, mainstream notions about each monitoring type. Overuse of a technology could arguably be a proxy for increased potential to violate privacy, and the low cost and simplicity of a GPS device (a concern, as mentioned earlier, that was

articulated by Justice Sotomayor in the United States v Jones, 2012) could make it prone to assumptions that it would be overused. Preconceptions about the effectiveness may also influence perceptions of potential privacy violations, for example, if one particular type of technology is generally thought to be much more effective than another, an assumption that law enforcement would want to use the new technology much more often than the other types could also increase the perception of potential privacy violation by that monitoring type. In fact, the difference in perceived effectiveness between Drones and Police tailing is mediated by perceptions of potential privacy violations and perceived effectiveness. This could be due in part to the possibility that people are less sure of what to expect from drones in terms of privacy violation and therefor also rely on perceptions effectiveness to guide decision about support.

When, in experiment two, we substitute the terms “GPS” and “Drone” with terms that are more generic, but maintain the essential features of each, indicate how each would be used, and state what type of information they would monitor, we see marked differences in terms of differential support and mediation. Both devices were described as covertly collecting information about the vehicle location during a specific time, but one purportedly attaches to the vehicle (like a GPS), while the other collects the information remotely without touching the car (like a Drone). Without altering the Police description and by ostensibly removing most preconceptions about “GPS” and “Drone”, the three monitoring types are no longer differentially support strictly by Type.

In addition to the absence of differential support for each monitoring

Type, these results also indicate that participants didn't base decision of support solely on the cost, nor did they base support decisions on the ability for suspects to evade the technology. However, there was an interesting interaction between the monitoring type and the relative cost of implementing it. Participants were more supportive of the "more expensive" Attached Device than the less expensive one. On the other hand participants were actually more in favor of the "less expensive", Police tailing than the "more expensive" Police tailing. The interaction was unremarkably in the case of the Unattached Device. One explanation for this Type by Cost interaction could be that participants believe more expensive Attached Devices would be used less often, posing of lower threat of privacy violation, thereby garnishing more support. At the same, the more expensive police officers might be perceived as being more motivated to uncover information than regular police officer, posing a greater threat of privacy violation and garnishing less support. If this were the case, however, we would have expected to see mediation by items that measured whether participants felt the monitoring type would be used often and/or if it would be effective, but neither of these factors showed signs of significant mediation. Two interesting factors did mediate this Type by Cost interaction: Private-space violation and general privacy violation, which brings the discussion back to United States v Jones.

The conflicting opinions from Justice Scalia and Justice Sotomayor about which Fourth Amendment precedent is more significant in determining how GPS surveillance threatens privacy, trespassing or violation of reasonable expectation

of privacy, may reflect the public's more complex underlying concerns about determining privacy violations. This would certainly be consistent with the fundamental role we expect the Supreme Court to play in our society. In which case, they both got it exactly right.

Recommendations

The research presented here is meant to initiate a strangely absent dialogue about the psychological nature of privacy. Certainly not a comprehensive examination of the mechanism guiding perceptions of privacy, it does highlight the complexities of experimentally examining privacy. Just as the study of morality found its footing in experimental research only after centuries of extensive legal and philosophical examination, it seems the time has come for privacy to also move beyond parenthetical lists of things that should or should not be protected and now be examined in terms of its social psychological roots and the mechanism by which it operates. Unless the essential principles of privacy can be experimentally defined it will remain unclear if the nature of privacy is changing with the emergence of new technologies or if there are indeed predictable and fixed rules that govern perceptions of privacy. Future research in this area should focus on investigating other potential mediators that might influence perceptions of privacy and private-space that would potentially lead to differential support for monitoring and surveillance techniques -not only those used by government agencies, but also those used by private organization. These factors might include manipulating the duration of the surveillance, manipulating the type of inferences that could be made about a person's identity by monitoring

type, manipulating who is collecting the information, manipulating the perceived benefits of collecting the information, and manipulating the amount of control a person has over the information. Progress in this area of research could help technology developers understand the impact that new information gathering technologies could have on human interests and could help guide governing bodies to get ahead of decision that impact privacy protection.

REFERENCES

Ackerman, S. (2012, March). CIA Chief: We'll spy on you through your dishwasher. *Wired.com*. Retrieved July 10, 2012, from http://www.wired.com/dangerroom/2012/03/petraeus-tv-remote/

Baker, D.B, Schweitzer, N.J. & Risko, E. (submitted). Neuroprivacy and the Self.

BBC News. (2012, January 31). Drones: What are they and how do they work. *BBC News*. Retrieved from http://www.bbc.co.uk/news/

Bilton, N. (2012, February 22). Behind the Google Goggles, Virtual Reality. *New York Times*, p. B1.

Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's Mechanical Turk: A new source of inexpensive, yet high-quality, data? *Perspectives on Psychological Science*, *6*(1), 3-5.

Costello, A. B., & Osborne, J. W. (2005). Best practices in exploratory factor analysis : Four recommendations for getting the most from your analysis. *Practical Assessment, Research & Evaluation*, *10*(7), 1–9.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104-115.

Eckholm, E. (2012, January 28). Private snoops find GPS trail legal to follow. *New York Times*, p. A1. New York.

Economist (2007, Dec 14). GPS changes direction tech.view. *Economist.Com / Global Agenda,*1-1. Retrieved from http://search.proquest.com.ezproxy1.lib.asu.edu/docview/208736847

Everett, M. (2003) The social life of genes: privacy, property and the new genetics. *Social Science & Medicine, 56*(1), 53-65.

Farah, M.J, Smith, M.E., Gawuga, C., Lindsell, D., Foster, D. (2009) Brain imaging and brain privacy: a realistic concern? *Journal of Cognitive Neuroscience* **325**, 119-27

Friedman, B. (2012, January 28). Privacy, technology and law. *New York Times*, p. SR5. New York.

Fiske, S. T., Kenny, D. a., & Taylor, S. E. (1982). Structural models for the mediation of salience effects on attribution. *Journal of Experimental Social Psychology*, *18*(2), 105–127. doi:10.1016/0022-1031(82)90046-4

Hayes, A. F. (2012). PROCESS: A versatile computational tool for observed variable mediation, moderation, and conditional process modeling [White paper]. Retrieved from http://www.afhayes.com/

Katz v. United States, 389 U.S. 347, 361 (1967).

Maass, P., & Rajagopalan, M. (2012, July 13). That's not my phone. That's my tracker. *New York Times*, p. SR5. New York.

Marx, G. T. (1989). *Undercover: Police Surveillance in America*. Berkley and Los Angelas, CA: University of California Press.

McLeod, S. (2008). Global Positioning System (GPS) Tracking. *Encyclopedia of Education Law*. Thousand Oaks, CA: Sage. Retrieved from http://sage-ereference.com.ezproxy1.lib.asu.edu/view/educationlaw/n166.xml?rskey=zOvv5k&result=2&q=Global Positioning System (GPS) Tracking

Nissenbaum, H. (1998). Protecting privacy in an information age: The problem of privacy in public. *Law and Philosophy*, *17*(5-6), 559-596.

Otterburg, A. A. (2004). GPS tracking technology: The case for revisiting Knotts and shifting the Supreme Court's theory of the public space under the Fourth Amendment. *Boston College Law Review*, *46*, 661–704.

Paolacci, G., Chandler, J., & Ipeirotis, P. G. (2010). Running experiments on Amazon Mechanical Turk. *Judgment and Decision Making*, *5*(5), 411-419.

Parker, R. B. (1973). A definition of privacy. *Rutgers Law Review*, *27*, 275-296.

Parent, W. A. (1983). Privacy, morality, and the law. *Philosophy and Public Affairs, 12*, 269-288.

Preacher, K. J., Rucker, D. D., & Hayes, A. F. (2007). Assessing moderated mediation hypotheses: Theory, methods, and prescriptions. *Multivariate Behavioral Research, 42*, 185-227.

Rand, D. G. (2012). The promise of Mechanical Turk: How online labor markets can help theorists run behavioral experiments. *Journal of Theoretical Biology*, *299*, 172-9. doi:10.1016/j.jtbi.2011.03.004

Schweitzer, N.J., Lovis-McMahon, D., Baker, D.A. (submitted). Don't say it's in the genes: Scientific determinism and responsibility.

Schweitzer, N.J., Saks, M.J, Murphy, E.R., Roskies, A.L., Sinnott-Armstrong, W., & Gaudet, L.M. (2011). Neuroimages as evidence in a mens rea defense: No impact. *Psychology, Public Policy, and Law. 17*(3), 357-393.

Shah, R. (2009). From beepers to GPS: Can the Fourth Amendment keep up with electronic tracking technology? *Journal of Law, Technology and Policy*, *29*(1), 281–294.

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

Suslak, B. A. (2011). GPS tracking, police intrusion, and the diverging paths of state and federal judiciaries. *Suffolk University Law Review*, *45*, 193–214.

Thrifty-Tel, Inc v. Bezenek, 46 Cal. App. 4th 1559 (1996).

Totenberg, N. (2011, January 7). Do police need warrants for GPS tracking Devices? *National Public Radio Online Podcast*. Retrieved from http://www.npr.org/ 2011/11/08/142032419/do-police-need-warrants-for-gps-tracking-devices

United States v. Knotts, 460 U.S. 276 (1993).

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

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

United States v. Pineda-Moreno, 617 F.3d 1120 (2010).

United States v Robinson 4:11 CR 361 AGF. (2011).

APPENDIX A

EXPERIMENT 1 – SCENARIO

Imagine that the Association of Police Chiefs is considering using **[Type]*** to follow suspects in order to obtain information that could lead to an arrest. **[Type description]**** to gather information about the vehicle's location during a particular period of time. Police departments can then compare this information with suspected criminal activity to determine any patterns of possible illegal activity. This technique would be implemented in such a way that no search warrant is needed for the police departments to conduct this type of surveillance, as it does not constitute a traditional search.

GPS condition

*…global positioning system (GPS) devices…

**A GPS device is covertly placed under a suspect's car…

Drone condition

*…drones…

** A drone is a small unmanned plane that covertly tracks a suspect from the air and is used…

Police Condition

* …full-time police officers…

**Police officers would covertly follow suspects in undercover cars…

APPENDIX B

QUESTIONS - EXPERIMENT 1 AND 2

1. If your state proposed this type of monitoring would you support it?

Follow-up questions presented in random order:

2. To what extent do you think that this type of monitoring seems reasonable?
3. To what extent do you believe that this type of monitoring should be legally permissible?
4. To what extent do you believe that this type of monitoring is a good idea?
5. To what extent do you believe that being monitored in this way would constitute a violation of the suspect's privacy?
6. To what extent do you believe that this type of monitoring would be a violation of the suspect's personal space?
7. To what extent do you believe that this type of monitoring would be used often by police departments?
8. To what extent do you believe that this type of monitoring would be abused?*
9. To what extent do you believe that this type of monitoring would pose a risk to bystanders?
10. To what extent do you believe that this type of monitoring would provide too many details about a person?
11. To what extent do you believe that this type of monitoring would help the police departments reduce crime?
12. To what extent do you believe that this type of monitoring would help catch/apprehend criminals?
13. To what extent do you believe that this type of monitoring will not provide enough information about a person?
14. To what extent do you believe that being monitored in this way would constitute a violation of your privacy?
15. To what extent do you believe that this type of monitoring would be a violation of the suspect's physical space?**

*Only appeared in question list for E1

**Only appeared in question list for Experiment 2

APPENDIX C

EXPERIMENT 2 – SCENARIOS

The Association of Police Chiefs is considering using **[Type]*** to follow suspects in order to obtain information that could lead to an arrest. **[Type description]**** gather information about the vehicle's location during a particular period of time. Police departments can then compare this information with suspected criminal activity to determine any patterns of possible illegal activity. This method is relatively **[Cost]*** and would cost police departments **[Cost description]**** than the current methods available. **[Type]*** are highly effective, **[Evade]*** this type of tracking. This technology would be implemented in such a way that no search warrant is needed for the police departments to conduct this type of surveillance, as it does not constitute a traditional search.

Type Manipulation (3)

Attached:

*Electronic Tracking Devices (ETD)

**An ETD is covertly placed under a suspect's car and is used to

Unattached:

*Remote Tracking Device (RTD)

**An RET device can remotely track a suspect's car without attaching anything to the vehicle and is used to

Police:

*full-time police officers

**Police officers would covertly follow suspects in undercover cars to

Cost (2)

Expensive

*expensive

**more money

Inexpensive

*inexpensive

**less money

Evade(2)

Possible

*but it is possible for a suspect to evade

Not Possible

*and it is not possible for a suspect to evade