Dissertation

Police, Process, and Privacy

Three Essays on the Third Party Doctrine

Anne E. Boustead

This document was submitted as a dissertation in August 2016 in partial fulfillment of the requirements of the doctoral degree in public policy analysis at the Pardee RAND Graduate School. The faculty committee that supervised and approved the dissertation consisted of Edward Balkovich (Chair), James Anderson, and Sasha Romanosky.

This work was funded by the James Q. Wilson Dissertation Fellowship at the Pardee RAND Graduate School.

PARDEE RAND GRADUATE SCHOOL

For more information on this publication, visit http://www.rand.org/pubs/rgs_dissertations/RGSD384.html

Published by the RAND Corporation, Santa Monica, Calif.

Abstract

Policymakers – state and federal, legislative and judicial – have expressed their interest in updating the laws regarding electronic surveillance. This interest is motivated by several recent trends. First, law enforcement surveillance has traditionally been limited as much by practical considerations, including the costs and technical difficulty of obtaining evidence, as legal ones. However, technological innovations have undermined these traditional practical protections, raising questions about the adequacy of the legal protections that remain. Second, law enforcement agencies are no longer the only entities collecting information about individuals. A wide variety of commercial entities now collect information about their customers, which law enforcement can access with only minimal legal protections. However, attempts to update electronic surveillance laws are made more difficult by the fact that very little is currently known about how law enforcement officers use electronic surveillance and commercial information requests.

In my dissertation, I present the results of three studies that investigate how law enforcement uses electronic surveillance. First, I quantitatively analyzed how restricting law enforcement access to particular types of third party information may change law enforcement use of one particular type of law enforcement surveillance – wiretaps. I find that state laws increasing protections for phone records decreased the duration of wiretap use, although it did not decrease the number of initial intercept requests. I theorize that increasing the legal protections for third party information may cause law enforcement officers to delay their use of wiretaps during investigations, as they need to gather more information before obtaining permission to use third party information.

Second, I qualitatively studied how law enforcement decides to use electronic surveillance and commercial information requests, identifying the factors law enforcement officers consider before deciding to use each technique. I find that there are significant practical barriers to using both electronic surveillance and third party information requests, although these barriers may be different.

Third, I analyze variation in local law enforcement agencies in the United States, and discuss how this variation may complicate attempts to address changes in practical protections against law enforcement surveillance. I conclude that there are several factors that may make it easier for law enforcement agencies that serve large communities to use electronic surveillance, when compared with law enforcement agencies that serve small communities. I then argue that failing to consider this variation when interpreting the Fourth Amendment in light of technological changes may create additional difficulties for smaller law enforcement agencies.

Acknowledgements

I would like to thank my dissertation committee for their endless patience, extensive feedback, and invaluable mentorship. This work has been immeasurably improved by their comments. I would also like to thank my external reader, Derek Bambauer of the University of Arizona College of Law, for his helpful insights from legal academia. This work was generously funded by the James Q. Wilson Dissertation Award. I am profoundly grateful for this support.

I would also like to thank the anonymous law enforcement officers who were willing to talk with me – sometimes at great length – about their electronic surveillance practices. I also owe a debt of gratitude to the numerous legal librarians who helped me navigate unfamiliar libraries and technology to access government reports published over forty years ago.

Finally, I would like to thank my family and friends for their patience and support during this time.

Table of Contents

Figures

Tables

Abbreviations

BJS	Bureau of Justice Statistics
CALEA	Communications Assistance for Law Enforcement Act
ECPA	Electronic Communication Privacy Act
FBI	Federal Bureau of Investigations
LEMAS	Law Enforcement Management and Administrative Statistics
UCR	Uniform Crime Reports

1. Introduction

"Three can keep a secret, if two of them are dead."
Benjamin Franklin

Privacy is a subject of both concern and contention. It has been described as "providing opportunities for political expression and criticism, political choice, and freedom from unreasonable police interference"[1] and as well as "self-assessment and experimentation."[2] According to one scholar, "[a] society without privacy protection would be suffocating, and it might not be a place in which most would want to live."[3] While discussions of privacy arise in a wide variety of legal and societal contexts,[4] I limit my discussion here to privacy as it pertains to Fourth Amendment protections against government surveillance.

While it has many benefits, "[p]rivacy comes at a cost."[5] Privacy is often discussed in terms of tradeoffs, especially in the context of privacy and governmental surveillance. Some have argued that privacy protections decrease the efficiency and effectiveness of law enforcement investigations. Expanding privacy protections, including Fourth Amendment rights "will have an impact on the ability of law enforcement to combat crime."[6] As President Obama explained, "it's important to recognize that you can't have 100 percent security and also then have 100 percent privacy and zero inconvenience."[7]

However, very little evidence is currently available on whether such tradeoffs occur in practice and, if so, the scope and extent of such tradeoffs. While it seems logical to conclude that expanding protections for individuals targeted by law enforcement surveillance may make certain types of information collection either more expensive or outright impossible, there are many unanswered questions that could aid policymakers in weighing the tradeoffs between privacy and security or privacy and law enforcement efficiency. How much more resources and manpower must law enforcement expend to collect a particular type of evidence if they must comply with stricter privacy protections? How many fewer arrests for a particular type of serious criminal activity will there be? How many fewer convictions? Answering these

---

[1] Stephen T. Margulis, *Privacy as a Social Issue and Behavioral Concept*, 59 J. Social Issues 243, 246 (2003).

[2] *Id.*

[3] Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 San Diego L. Rev. 745, 762 (2007).

[4] *See*, *e.g.*, Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477 (2006).

[5] *Riley v. California,* 134 S. Ct. 2473, 2493 (2014).

[6] *Id.*

[7] *Statement by the President* (2013), https://www.whitehouse.gov/the-press-office/2013/06/07/statement-president (last visited Sept. 15, 2016).

questions would allow policy makers to frame the discussion around potential new privacy protections in terms of costs and benefits, instead of rhetoric and anxiety.

These questions likely remain unanswered because of the profound difficulty of addressing them. Criminal investigations are complex, and law enforcement officers often pursue evidence from multiple sources. New privacy protections may impact not only the type of surveillance at issue, but also other surveillance techniques that rely on the information obtained from the original type of surveillance. For example, there has been great interest from both policy makers and the public in further regulating law enforcement access to commercially collected data, including proposed legislation at both the state and federal level.[8]

However, as law enforcement access to commercially-collected data becomes more difficult, it may in turn become more difficult for law enforcement to use forms of surveillance that require prior access to commercially collected data. For example, law enforcement generally must present evidence from phone records in order to obtain permission to wiretap a phone line; increasing the difficulty of obtaining phone records may also increase the difficult of obtaining wiretap authorization. Discussions of how proposed privacy protections may impact security and efficiency should take into account the complex nature of criminal investigations and the potential relationships between different forms of surveillance.

The problem of complexity is compounded by the lack of available statistics on electronic surveillance use. No quantitative data are available on many forms of electronic surveillance use; the data that are available are often highly aggregated and only describe the last few years. For example, while companies have recently started publishing transparency reports describing the number of requests for information they have received from government officials, these reports frequently provide data on the national level, making evaluation of state-level policy experimentation impossible.[9] One notable exception to this trend is the *Wiretap Reports* published by the Administrative Office of the U.S. Courts. These reports are publicly available,[10] and provide detailed information about each wiretap request made by federal, state, and local law enforcement since 1968.

In sum, the current debate over privacy and electronic surveillance centers on largely untested assumptions about the relationship between privacy protections and other important social goods, particularly security and efficiency of law enforcement investigations. In order to

---

[8] *Email Privacy Act*, H.R. 699, 114th Cong. (2016). Some states have managed to successfully pass additional regulations of third party data. *See* S.B. 651 (Cal. 2016).

[9] *See*, *e.g.*, Google*, Transparency Report*, https://www.google.com/transparencyreport/. This report provides information on the country level, for six-month periods beginning in July 2009.

[10] Editions of the *Wiretap Report* published after 1996 are available on the Administrative Office of the U.S. Courts' website. *See* U.S. Courts, *Wiretap Report*, http://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports. Although they are publicly available, editions of the *Wiretap Report* published from 1968-1996 can only be accessed through the federal deposit library system.

test these assumptions, information is needed about how law enforcement officers use electronic surveillance, and how this use is affected by new proposals to protect individual privacy. Such information could help policy makers, advocates, and the general public engage in a more productive discussion about the benefits and costs of privacy protections.

Overview of Document

My primary objective is to provide evidence regarding how surveillance is used by domestic law enforcement in the United States. While there is strong evidence to suggest that electronic surveillance use has become more prevalent in recent years, the context of this apparent increase has not been well explored. This is particularly problematic because an increase in electronic surveillance use does not necessarily imply that law enforcement is using electronic surveillance in an abusive or unconstitutional manner. In fact, some law enforcement officers have suggested that the increase in electronic surveillance may be due to the increased adoption of electronic communication devices and counter-surveillance technologies.[11] Without further information, it is extremely difficult to understand whether and how electronic surveillance use may threaten privacy rights. I meet this objective by studying electronic surveillance use from three perspectives: qualitative, quantitative, and legal. My dissertation is therefore comprised of three papers, each analyzing law enforcement use of surveillance from a different perspective.

In my first paper, I quantitatively study how law enforcement has used one particular form of surveillance: wiretaps. Using data from the Wiretap Reports published annually by the Administrative Office of the U.S. Courts, I study the impact of state-level laws strengthening protections against law enforcement use of third party information on wiretap requests. I hypothesize that law enforcement may be less able to use wiretaps when it becomes more difficult for them to collect the evidence necessary to make a successful wiretap request. My findings indicate that some measures of wiretap use do indeed decrease after a state rejects the third party doctrine with respect to phone record information, providing the first evidence that regulation of law enforcement use of third party information may affect their use of other forms of surveillance.

In my second paper, I explore law enforcement use of electronic surveillance qualitatively, in order to better understand what factors govern law enforcement use of electronic surveillance. I am particularly interested in differentiating between the factors that law enforcement considers when deciding to use traditional forms of electronic surveillance and those factors they consider when deciding to request information from a commercial entity. As technological changes have allowed (and will continue to allow) law enforcement to obtain increasing amounts of

---

[11] James B. Comey, *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? Remarks to the Brookings Institution* (2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course (last visited Sept. 15, 2016).

information from commercial entities, identifying and understanding the barriers to requesting commercial information will help determine what policies should govern law enforcement access to these data sources. I find five factors that law enforcement officers appear to consider when deciding to use electronic surveillance and commercial information requests: legal concerns, resource concerns, investigatory concerns, safety concerns, and information concerns. These additional concerns suggest that law enforcement officers may face previously unrecognized barriers that law enforcement officers may face when using electronic surveillance and commercial information requests, and suggest additional levers that policymakers may use to regulate these techniques.

Finally, in my third paper, I analyze law enforcement use of electronic surveillance from a legal perspective, focusing on how variation in law enforcement agencies may affect how technological innovations change law enforcement surveillance. Both policymakers and academics have expressed concern that technological innovations may be undermining long standing practical protections for individuals targeted by law enforcement surveillance; some have suggested increasing legal protections to compensate for this loss. I argue that increasing practical protections without accounting for variation across different types of police departments may lead to unintended consequences, as smaller departments that are less able to adapt to changing technology may be unduly affected by these increased protections.

I conclude by discussing several overarching policy concerns that arose during this research. In particular, I address the current debate over whether electronic surveillance is "going dark" or entering a "golden age." I also argue that electronic surveillance policy should be based on an understanding of how electronic surveillance is conducted in practice, rather than summary statistics on how the "amount" of electronic surveillance has changed over time. I then offer some concrete policy lessons for both legislative and judicial policy makers.

2. Does Rejection of the Third Party Doctrine Change Use of Electronic Surveillance? Evidence from the Wiretap Reports.[12]

Abstract

Under an aspect of Supreme Court jurisprudence known as the third party doctrine, the Supreme Court has determined that Fourth Amendment protections do not apply when law enforcement seeks information that an individual has shared with a third party. This doctrine has been widely criticized, and several states have rejected it by holding that their state constitution provides additional protection to individual rights. However, little research has been done on how rejection of the third party doctrine has affected law enforcement behavior. Understanding how law enforcement investigations are changed by rejection of the third party doctrine would provide crucial information about the inherent tradeoffs between individual Fourth Amendment rights and pubic safety. Without a clearer understanding of how law enforcement chooses between different types of investigative techniques, the effects of shifting Fourth Amendment protections are perilously unclear.

In this paper, I explore how state law enforcement use of electronic surveillance is affected by legal protections for third party information. I provide evidence for this phenomenon in the instance of communications intercepts and third party information requests. Specifically, I analyze whether use of communications intercepts changes when state supreme courts hold state law enforcement must demonstrate probable cause before obtaining third party information. I obtain data about state protections for third party information by analyzing state supreme court opinions rejecting the third party doctrine, and obtain information about communication intercepts from the *Wiretap Reports*. I seek to discover whether rejection of the third party doctrine causes law enforcement to change their use of communications intercepts and, if so, whether communications intercepts use increases or decreases. I find that rejecting the third party doctrine changes law enforcement use of communications intercepts. Before considering the type of information protected by rejection of the third party doctrine, it appears that rejecting the third party doctrine does not decrease the number of initial law enforcement requests for communications intercepts, but does decrease both the overall number of requests for communications intercepts and the total number of days of interception authorized. Once the

[12] This work was funded by the James Q. Wilson Dissertation Fellowship at the Pardee RAND Graduate School. I would like to thank my Ed Balkovich, Sasha Romanosky, James Anderson, and Derek Bambauer for their valuable comments and feedback. I would also like to thank participants from the 2016 Western Empirical Legal Studies Conference, American Law & Economics Society Annual Meeting, and Privacy Law Scholars Conference for their helpful questions and suggestions.

type of information protected by rejection of the third party doctrine is considered, it appears that only additional protections for phone records change law enforcement use of communications intercepts. Rejecting the third party doctrine with respect to phone records decreases the overall number of communications intercepts and the total days of interception authorized, but not the number of initial communications requests. I conclude by discussing the significance of my results.

I. Introduction and Background

Both judicial and legislative policymakers have long struggled with the tradeoff between protecting public safety by allowing law enforcement broad power to investigate crime, and ensuring individual privacy by limiting invasive law enforcement practices. It has proven particularly difficult to strike a balance between these competing interests when technological innovations change the tools that law enforcement can use to investigate crimes (Kerr, 2011). On one hand, electronic surveillance has become a crucial tool in investigating a wide variety of crimes, especially narcotics crimes (Nunn, 2008). On the other hand, electronic surveillance may undermine long-standing expectations about the privacy of activities and communications, and expand the government's ability to obtain information about its citizens in a way that facilitates overreaching and even abuse (Bernstein, 1976).

The Fourth Amendment, which protects "[t]he right of the people to be secure…against unreasonable searches and seizures"(U.S. Const. Amend. IV), plays a critical role in regulating how law enforcement investigates crimes. Under the modern approach, law enforcement actions are only regulated by the Fourth Amendment if they violate a reasonable expectation of privacy (*Katz v. United States*, 389 U.S. 347, 361 (1967)).[1] While there is no clear formula for determining whether law enforcement conduct has violated a reasonable expectation of privacy, courts often look to whether the conduct impacted a place that traditionally enjoyed Constitutional protection and the type of information sought (Kerr 2007), as well as "whether the government's intrusion infringes upon the personal and society values protected by the Fourth Amendment" (*Oliver v. United States*, 466 U.S. 170, 182-3 (1984)). If this condition is met, then the law enforcement action is described as a "search" and Fourth Amendment protections apply (*U.S. v. Jones*, 565 U.S. 945 (2012), *Florida v. Jarines*, 569 U.S. 1 (2013)).

If law enforcement wants to undertake a search, then officers must generally first obtain a warrant by presenting an independent judicial officer with probable cause (*Payton v. New York*, 445 U.S. 573 (1980)). Although some research suggests that cost may limit the use of searches more than requiring a warrant based on probable cause (Minzner and Anderson 2013), the warrant clause has been one of the most fundamental protections for those targeted by governmental surveillance since adoption of the Fourth Amendment.[2]

---

[1] That is not to say that physical intrusion is irrelevant to the issue of whether law enforcement has violated a reasonable expectation of privacy. As was recently noted by the Supreme Court in *U.S. v. Jones*, *Katz* did not change the long-standing historical understanding that "the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ("persons, houses, papers, and effects") it enumerates." *U.S. v. Jones*, 132 S. Ct. 945, 950 (2012).

[2] However, there are exceptions to the warrant requirement. Perhaps the most frequently used exception to the warrant requirement is the exception for a search incident to an arrest. When law enforcement arrests an individual, they may search the individual's person and "the area into which an arrestee might reach" in order to find weapons that might pose a threat to law

However, the term "search" has been specifically defined by the Supreme Court in a way that excludes many activities that could colloquially be described as searches.[3] Under the third party doctrine, an individual does not have a reasonable expectation of privacy in information they have shared with a third party. Therefore, it is not considered a search when, for example, law enforcement obtains an individual's phone records from their telephone service provider (*Smith v. Maryland*, 442 U.S. 735 (1978)), or their financial records from their bank (*United States v. Miller*, 426 U.S. 435 (1976)). Some states have rejected the third party doctrine by holding that their state constitution provides additional protections for individual rights (Henderson 2006). Rejection of the third party doctrine might affect not only how law enforcement decides to use third party information, but also how they conduct other forms of surveillance – and, in turn, the effectiveness and efficiency of criminal investigations.

A hypothetical may demonstrate how rejecting the third party doctrine can affect the course of a criminal investigation. Assume that a local law enforcement officer in Arizona is investigating a narcotics distribution network. After identifying a potential suspect, the Arizona officer wants to intercept the suspect's phone calls to confirm the suspect's involvement with the distribution network, identify other persons involved, and obtain information about how the narcotics distribution network is operated so that he can build a case against the whole cartel. Since the officer must demonstrate "probable cause to believe that particular communications concerning [the] offense will be obtained through the interception" to obtain judicial permission to use a communications intercept (ARS 13-3010), the officer will usually first seek to obtain the suspect's phone records to demonstrate that the phone is being used to communicate with other members of the narcotics network. In Arizona, state and local law enforcement can obtain phone records without first obtaining a warrant based on probable cause. Instead, the officer need only be able to show that "the information likely to be obtained is relevant to an ongoing criminal investigation" (ARS 13-3017) – a much easier standard to meet than probable cause. The officer is able to obtain phone records relatively early in his investigation, and therefore can begin to use communications intercepts more quickly.

However, a local law enforcement officer in Colorado investigating a similar crime faces a different set of legal restraints on his ability to use third party information. Like the officer in Arizona, the Colorado officer wants to intercept his suspect's phone calls so as to investigate the narcotics distribution network operating in his state. Because he must also demonstrate

---

enforcement or evidence which might be destroyed (*Chimel v. California, 395 U.S. 752, 763 (*1968)). Law enforcement can also conduct a search without a warrant if they have appropriate consent (*United States v. Matlock*, 415 U.S. 164 (1973)) or seize items they see in plain view if they have probable cause to believe these items are evidence or contraband (*Arizona v. Hicks*, 480 U.S. 321 (1986)).

[3] Because it is used as a term of art in criminal procedure law, throughout this discussion I only use the word "search" to refer to activities that constitute searches for purposes of the Fourth Amendment.

"probable cause for belief that particular communications concerning [the] offense will be obtained through the interception" before being granted judicial permission to use a communications intercept (CRS 16-15-102), the Colorado officer has the same incentives to first request the suspect's phone records. However, unlike Arizona, Colorado has rejected the third party doctrine by holding that law enforcement must demonstrate probable cause to obtain phone records (*People v. Sporleder*, 666 P.2d 135 (Colo. 1983)). The officer in Colorado must therefore expend additional time and resources to meet this higher legal burden before he can request phone records – assuming that he is able to meet it at all. Because it is more difficult for him to obtain critical evidence supporting his request to use a communications intercept, the officer may be less likely to use a communications intercept or may only be able to use it later in his investigation.

As is shown by these hypotheticals, rejecting the third party doctrine may alter how law enforcement uses different forms of surveillance over the course of an investigation. However, no one has empirically studied the effects of rejecting the third party doctrine on law enforcement surveillance. This research is imperative for two reasons. First, as improvements in consumer technology have increased the amount of personal information routinely shared with third party commercial entities, the third party doctrine has become an expansive and extensively criticized[4] gap in Fourth Amendment protections. There are indications that the Supreme Court may soon "reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties" (*United States v. Jones*, 132 S.Ct. 945,957 (2012)(Sotomayor, J., concurring)). Without additional research, it is difficult to predict how rejection of the third party doctrine on the national level will affect law enforcement's ability to investigate crime efficiently.

More fundamentally, however, rejecting the third party doctrine increases the privacy rights available to individuals, by limiting the actions that law enforcement can undertake before seeking a warrant. The Fourth Amendment, "as least as conventionally understood, confronts us with the problem of balancing effective law enforcement and personal privacy" (Wasserstrom and Seidman, 1998 p. 30). However, there is currently little evidence about how increasing protections for individual rights affects law enforcement activities, and consequently the balance established by the Fourth Amendment. This is an empirical question and, if possible, should be answered with empirical evidence.

In this paper, I investigate the cost, in terms of lost law enforcement activities, of expanding protections for third party information in one particular context. I look specifically at whether and how rejecting the third party doctrine changes law enforcement use of one particular form of surveillance – communications intercepts. I seek to answer two questions: First, does rejection of the third party doctrine – either under any circumstances or with respect to a particular type of

[4] It has been described as "fundamentally misguided" (Henderson 2011, p. 40) and "ill suited to the digital age" (*United States v. Jones*, 132 S.Ct. 945, 957 (2012)).

information – cause law enforcement to change their use of communications intercepts? Second, if rejection of the third party doctrine causes law enforcement to change their use of communications intercepts, does it cause intercept use to increase or decrease? Drawing from the economic theory of complement and substitute goods, I hypothesize that law enforcement will change their rate of intercept use in response to rejection of the third party doctrine. However, the direction of the change will depend on the relationship between the use of communications intercepts and the use of third party commercial information.

To test these hypotheses, I exploit variation in state rejection of the third party doctrine. I then conduct three analyses to examine how increasing barriers to law enforcement use of third party information affects use of communications intercepts. First, I conduct preliminary graphical analyses to explore whether states that reject the third party doctrine use communications intercepts differently from states that do not reject the third party doctrine. This analysis may provide preliminary evidence for my hypotheses, but cannot demonstrate causality. Second, I employ difference-in-difference analysis to determine whether state court rejection of the third party doctrine changes law enforcement use of communications intercepts. Difference-in-difference analysis allows for unbiased estimates of the effect of rejecting the third party doctrine on wiretap rates,[5] provided that certain key assumptions[6] are met (Conley and Taber 2011). By comparing differences in use of communications intercepts before and after rejection of the third party doctrine, this analysis provides evidence of causality. Third, I test the robustness of my results to changing the variables that describe rejection of the third party doctrine to account for state statutes providing similar protections, and eliminating all states whose supreme courts never address whether or not their constitution provides protections to third party information.

I find that rejecting the third party doctrine changes law enforcement use of communications intercepts. Before considering the type of information protected by rejection of the third party doctrine, it appears that rejecting the third party doctrine does not decrease the number of initial[7]

---

[5] In other words, using difference-in-difference analysis ensures that, on average, the estimated effect of the third party doctrine on use of communications intercepts is the same as the actual effect.

[6] In particular, the difference-in-difference estimator will be unbiased in this instance if, among other things, use of communications intercepts does not change differentially over time between the treatment and control groups.

[7] An initial request refers to the first request made by an officer; the overall number of requests refers to both the initial request and any requests to extend that authorization. Since judicial authorization to use a wiretap may not last for longer than 30 days, the officer must seek an extension to continue using the wiretap after that time. For example, say an officer requests (and is granted) permission to use a wiretap for thirty days, and then seeks (and is granted) permission to extend use of the wiretap twice, each for an additional thirty days. Under the metrics described above, this situation would count as one initial request and three overall requests.

law enforcement requests for communications intercepts, but does decrease both the overall number of requests for communications intercepts and the total number of days of interception authorized. Once the type of information protected by rejection of the third party doctrine is considered, it appears that only additional protections for phone records change law enforcement use of communications intercepts. Rejecting the third party doctrine with respect to phone records decreases the overall number of communications intercepts and the total days of interception authorized, but not the number of initial communications requests.

In the next section, I develop an argument for why rejecting the third party doctrine might affect law enforcement use of communications intercepts, drawing on the theory of complement and substitute goods. In the following sections, I describe my data and methodology, and then present my results. I conclude by discussing the policy implications of this work.

II. Effect of Rejecting the Third Party Doctrine on Law Enforcement Use of Communications Intercepts

A. Lessons from Economics: Complement and Substitute Goods

Economists have long studied how the consumption of certain goods may affect consumption of other goods. Assuming that a consumer has a fixed budget, then utility maximization theory suggests that they will select their consumption of goods in order to maximize their utility without overspending their budget. When the price of a particular good rises, consumers will generally reallocate their consumption by substituting other goods for the now more expensive good (Shocker, Bayus, and Kim 2004). For example, if a consumer can get the same utility from consuming either coffee or tea, increasing the cost of coffee will increase consumption of tea, as the consumer trades consumption of coffee for the less expensive alternative of tea.

On the other hand, consumers do not always trade off consumption of goods in this manner. Sometimes, certain goods provide a consumer with more utility when consumed with other goods. Goods that are related in this way are known as complements, and increasing the cost of one will decrease consumption of the other (Drahos, 2004). For example, paint and paintbrushes might be considered complementary goods, as a consumer gets more utility from using them together. If the cost of paint increases, then the consumption of paintbrushes might be expected to decrease.

Just as consumers make decisions about what goods to purchase, law enforcement officers make decisions about what types of investigative techniques to use. Assume that law enforcement officers are rational actors who derive utility from obtaining incriminating evidence about a particular crime (Minzner and Anderson 2013). They are able to select between various types of investigative techniques in order obtain this evidence, subject to both budget and legal constraints. When a state supreme court rejects the third party doctrine, they increase the cost of obtaining third party information in two ways. First, law enforcement must now comply with

more comprehensive legal processes, such as obtaining a warrant instead of a court order. Second, law enforcement must be able to demonstrate a higher quantum of proof before they can obtain the relevant legal process. Even assuming that sufficient evidence is available for law enforcement to meet this higher level of proof, gathering more extensive evidence requires a higher expenditure of law enforcement resources. As the price of obtaining third party data increases, law enforcement utilization of other investigative techniques may also be changed. However, the direction of this change will depend in part on whether law enforcement uses third party data requests and other investigative techniques and complements or substitutes.

B. Does rejecting the third party doctrine increase or decrease law enforcement use of communications intercepts?

The third party doctrine has been used to justify allowing law enforcement access to a wide range of information without a warrant. However, judges in a particular case do not apply or reject the third party doctrine wholesale. Rather, a judge is presented with a case that requires him to determine whether the third party doctrine should apply to a particular type of information. Therefore, states may reject the third party doctrine with respect to some types of information and not reject it with respect to others. Restrictions on different types of information may affect law enforcement behavior differently. Therefore, in this section, I draw from the economic theory of complement and substitute goods to discuss why rejection of the third party doctrine with respect to three distinct types of third party information – phone records, bank records, and location information – may increase or decrease law enforcement use of communications intercepts.

1. Phone Records

There are several reasons why making it more difficult for law enforcement to obtain phone records may reduce use of communications intercepts. Most significantly, restricting access to phone records makes it more difficult for law enforcement to meet the legal requirements for using communications intercepts under Title III. As phone records include information about calls made to and from a particular phone line, they may be virtually mandatory to demonstrate that the phone law enforcement wants to target is being used in the commission of a crime or by those who have committed the crime, a mandatory component of obtaining authorization to intercept communications. Phone records requests can also link a suspect to the commission of a crime by showing that he is communicating with others who are known to be involved in the crime.

Additionally, rejecting the third party doctrine with respect to phone records may reduce the resources available for law enforcement to conduct communications intercepts. Communications intercepts require significant manpower, and manpower is a limited resource. If it becomes more difficult for law enforcement to obtain phone records, they may be more sensitive to the cost of communications intercepts.

Finally, rejecting the third party doctrine with respect to phone records may make it more difficult for law enforcement to realize that suspects are communicating with each other. Consequently, law enforcement may be less aware that the contents of communication will reveal useful information. Since law enforcement considers the type of information collected when deciding to use electronic surveillance, this may reduce use of communications intercepts.

2. Bank Records

Restricting law enforcement access to bank records may make it more difficult for law enforcement to demonstrate that particular individuals are involved in a crime. Financial records may demonstrate a connection between two people, or provide evidence of motive in a financially driven crime. However, bank records are unlikely to provide persuasive evidence that a particular phone line is being used to discuss criminal activity, a necessary component of obtaining permission to use a communication intercept. Therefore, the connection between bank records and communications intercepts may not be as clear as the connection between phone records and communications intercepts.

Additionally, increasing the legal barriers to obtaining bank records may reduce the resources available for law enforcement to obtain the contents of communication. If law enforcement has to expend more resources on obtaining bank records, they may be more sensitive to the cost of communications intercepts and consequently use them less.

3. Location Information

It is unclear whether location information is a complement or substitute for communications intercepts. Location information may help law enforcement develop the probable cause required to use a communications intercept by providing information about a suspect's activities and relationships. Restricting access to location information may therefore make it more difficult for law enforcement to use communications intercepts, and consequently decrease their prevalence.

However, restriction of location information could also increase law enforcement use of communications intercepts. When deciding to use electronic surveillance, law enforcement may consider the context of their investigation, including whether there are alternative methods of obtaining the information they require. Because location information provides incredibly powerful data about an individual's travel, habits, and relationships, law enforcement may view location information as an acceptable alterative to communications intercepts. Under these circumstances, restricting access to location information may make it less attractive to law enforcement, and consequently increase use of communication intercepts.

III. Prior Literature

Fourth Amendment protections have been the subject of extensive academic work. Much of this work deals with the normative basis of Fourth Amendment law (Ku 2002; Amar 1994) and suggestions for the adoption of the Fourth Amendment to novel situations and technologies (Kerr

2001; Owsley 2013). In particular, the third-party doctrine has been exhaustively critiqued: "[a] list of every article or book that has criticized the doctrine would make . . . the world's longest law review footnote" (Kerr 2009, 563). However, little empirical work has been done on the effects on Fourth Amendment law on public expectations, police behavior, or crime. One notable exception is Slobogin and Schumacher (1993) who asked members of the general public to "gauge the impact of police investigative techniques on their privacy and autonomy" (Slobogin and Schumacher 1993, 732). They used the results of this survey to rank the perceived intrusiveness of fifty investigative techniques; they found that "[m]onitoring phone for 30 days" was perceived to be very intrusive, while "[p]erusing bank records" and "[u]sing a beeper to track car" were less invasive (Slobogin and Schumacher 1993, 738-9).

Additionally, while there is a rich body of literature on law enforcement decision making, little work has been done on how law enforcement makes decisions regarding electronic surveillance. Minzner and Anderson (2013) investigate how the warrant requirement affects law enforcement use of communication intercepts, concluding that the expense of obtaining and implementing an intercept request limits law enforcement use of communication intercepts more than legal protections. Instead, researchers have developed frameworks to explain how law enforcement officers decide whether to use force (Terrill and Mastrofski 2002) and whether to make an arrest in a domestic violence situation (Kane 1999; Phillips and Sobol 2010). While researchers have considered law enforcement decision making in the context of searches and seizures, these studies have generally been limited to in-person searches and interrogations. Decisions to engage in "stop and frisk" and "traffic stop" interactions have been well studied, particularly with regards to the role racial profiling might play in the decision making process (Smith and Petrocelli 2001; Schafer et al. 2006; Ridgeway 2007).

The lack of research into how law enforcement uses electronic surveillance is probably due in large part to the lack of quantitative data about electronic surveillance use. However, some scholars have begun to use wiretap data to investigate issues related to electronic surveillance use. Minzner and Anderson (2013), discussed above, uses the Wiretap Reports to investigate the role of the warrant requirement in the decision to use communication intercepts. In their book *Privacy on the Line: The Politics of Wiretapping and Encryption*, Diffie and Landau (1998) described broad trends in the Wiretap Reports in order to understand wiretap use. However, they only calculated summary and descriptive statistics, and did not attempt to relate wiretap use in a particular jurisdiction to the underlying characteristics of that jurisdiction. Nunn (2008) used the data contained within the Wiretap Reports to analyze trends in the productivity of Title III wiretaps, as quantified by the number of intercepted communications, total arrests, and total convictions. However, he neither looked at differences in wiretap productivity between different states nor the impact of state level characteristics on productivity. To my knowledge, however, no one has yet used the Wiretap Reports to study the relationship between law enforcement use of different types of electronic surveillance.

IV. Data and Methods

A. Description of Data

1. State Supreme Court Rejection of the Third-Party Doctrine

I began by developing a dataset describing state supreme court decisions concerning whether their state constitution protected third party information. To do this, I started with a list of state supreme court cases that had cited the Supreme Court cases establishing the third party doctrine and applying it to particular types of information.[8] Because it is highly implausible that a state supreme court would depart from the Supreme Court's holding that a reasonable expectation of privacy exists in a particular type of information without discussing the existing Supreme Court precedent, this is an effective and efficient way of identifying relevant case law.

After selecting these seminal Supreme Court cases concerning the third party doctrine, I used Lexis' Shepard's Summary to determine which state courts had issued decisions citing each opinion. I first eliminated each case that had not been issued by a state supreme court before January 1, 2012, and then eliminated cases that did not concern law enforcement searches for phone records, business records, or location information. I then coded each relevant case based on whether the state supreme court held that their constitution protected each type of third party information, or whether no such protections existed. This case selection process is described in Table 2.1 below.

Table 2.1. Description of Case Selection Process

Supreme Court Case	Citation	N State Cases	N State S. Ct. Cases	N Relevant Cases	Percent Relevant	Median Case Year
Smith v. Maryland	442 U.S. 735 (1979)	779	168	28	16.67%	1987
United States v. Miller	425 U.S. 435 (1976)	320	89	30	33.71%	1992
United States v. Knotts	460 U.S. 276 (1983)	189	43	5	11.63%	1988
Total		1140	257	45	17.51%	1989

This table describes the results of legal research used to identify state case law related to the third party doctrine. Three seminal cases related to the third party doctrine were selected, and then Lexis was used to narrow down a list of state supreme court cases that cited these decisions. State supreme court cases were defined as any opinion from the highest court in each state, excluding the District of Columbia. The cases were then reviewed to determine whether they were relevant to the application of the third party doctrine to phone records, business data, or location data. The results from each case do not sum to the total, because some cases cited more than one Supreme Court case.

[8] Because I focus on the impact of access to phone records, business records, and location information on law enforcement's decision to use electronic surveillance, I selected those cases where the Supreme Court held that these types of information were not protected by the Fourth Amendment: *Smith v. Maryland*, 442 U.S. 735 (1978), *United States v. Miller*, 425 U.S. 435 (1976), and *United States v. Knotts*, 460 U.S. 276 (1983).

While completing this coding, I also noted any citations to relevant state supreme court decisions that did not show up in my prior search. I found three such cases,[9] and included them in my analysis. I then confirmed my coding by comparing my results to the description of case law provided in Henderson (2006). Where my coding contradicted the description provided in Henderson (2006), I reviewed my data and updated accordingly.

An overview of which state supreme courts addressed the third party doctrine under their state constitution, including the year in which these decisions were decided and whether state constitutional protections were provided to third party data, can be found in Table 2.2 below. Twelve states have rejected the third party doctrine as applied to phone records, bank records, or location information, while 12 state supreme courts considered whether their constitution protected third party information, but explicitly held that it did not. Because state supreme courts may hold that their constitutions protect some forms of third party information but not others, these groups are not mutually exclusive. For example, Hawaii provides state constitutional protections to phone records, but not bank records. Further details regarding these cases, including the case name, citation, and relevant text, are provided in Appendix B.

Table 2.2. State Supreme Court Case Law Regarding the Third Party Doctrine

	Reject Third Party Doctrine				Did Not Reject Third Party Doctrine			
State	***Any***	***Phone Records***	***Bank Records***	***Location Information***	***Any***	***Phone Records***	***Bank Records***	***Location Information***
Alabama								
Alaska								
Arizona								
Arkansas								
California	1974	1979	1974					
Colorado	1980	1983	1980	1985				
Connecticut								
Delaware					1984	1984		
Florida	1985	1989	1985					
Georgia								
Hawaii	1989	1989			1990		1990	
Idaho	1989	1989						
Illinois								
Indiana					1980	1980		
Iowa								
Kansas					1993	1993	1993	
Kentucky								
Louisiana								
Maine								

[9] These cases were *Burrows v. Superior Court*, 529 P.2d 590 (Cal. 1974), *Commonwealth v. Murtha*, 465 A.2d 783 (Pa. 1984), and *Shaktman v. State*, 553 So.2d 148 (Fla. 1989).

State	Reject Third Party Doctrine				Did Not Reject Third Party Doctrine			
	Any	*Phone Records*	*Bank Records*	*Location Information*	*Any*	*Phone Records*	*Bank Records*	*Location Information*
Maryland					1978	1978		
Massachusetts	2009			2009	1998	1998		
Michigan								
Minnesota								
Mississippi								
Missouri								
Montana					1982	1982		
Nebraska								
Nevada					2002			2002
New Hampshire					1987	1987		
New Jersey	1982	1982	2005					
New Mexico								
New York	2009			2009	1982	1982		
North Carolina								
North Dakota					2011		2011	
Ohio					1994	1994		
Oklahoma								
Oregon	1988			1988				
Pennsylvania	1979	1989	1979					
Rhode Island								
South Carolina								
South Dakota								
Tennessee								
Texas								
Utah	1991		1991					
Vermont								
Virginia								
Washington	1986	1986	2007	2003				
West Virginia								
Wisconsin								
Wyoming					1979	1993	1979	
N States	12	8	7	5	13	10	4	1
Median Year	1987	1987	1985	2003	1987	1985	1991	2002

This table describes the year in which each state supreme court either rejected or affirmative accepted the third party doctrine. If a state supreme court addressed this issue more than once, then the year of the first decision is provided. Additional information, including case names and citations for each decision, can be found in Appendix B.

After coding the relevant case law, I constructed a dataset describing whether each state had rejected the third party doctrine for each year included in my analysis. To ensure consistency in coding, each state-year was coded as rejecting the third party doctrine only if the state supreme court had held that their constitution protected the third party data in question prior to January 1st

of that year. In other words, state supreme court decisions protecting third party data do not appear in this dataset until the start of the year after they were decided. Summary statistics are provided in Table 2.3 below.

Table 2.3. Summary Statistics for Third Party Doctrine Data

	Rejection of TPD for Information Type						
Type of Information	***N States***	***Percent States***	***N State-Years***	***Percent State-Years***	***Year of First Case***	***Year of Last Case***	***Median Year***
Phone Records	8	16.0%	210	10.2%	1979	1989	1987
Bank Records	7	14.0%	163	7.9%	1974	2007	1985
Location Information	5	10.0%	66	3.2%	1985	1985	2003
Any	12	24.0%	283	13.8%	1974	2007	1987

This table summarizes the dataset describing state supreme court rejection of the third party doctrine.

2. Wiretap Data

Federal law requires judges who hear requests for intercept orders and the prosecutors who request such an order to report certain information to the Administrative Office of the U.S. Courts (18 U.S.C. § 2519 (2015)). The Administrative Office of the U.S. Courts then compiles this information, and publishes it yearly in a series of documents commonly referred to as the *Wiretap Reports*, which contain detailed information about each communication intercept order requested.[10] I obtained the reports from 1997-2011 through the Administrative Office's website, and the reports from 1972-1996 from various online repositories and federal deposit libraries. Because the reporting of communication intercept requests is often delayed to a year after the request was made,[11] I confined my analysis to the years 1972-2012 to ensure the data were relatively complete, and looked only at those requests made in state court to state judges. This process resulted in 40,231 observations, each related to a different communication intercept request.

[10] The Wiretap Reports include information on the jurisdiction in which the request was made, the judge who heard the request, the prosecutor who made the request, the highest offense under investigation, the date of the application, the length of the order, whether the order was extended, and the type and location of the intercept. Based on supplemental information provided by prosecutors, the reports also contain information about the results of each wiretap order, including the number of intercepts, incriminating intercepts, and persons intercepted, the cost of executing the order, the arrests, trials, and convictions associated with each order, and motions to exclude evidence from the wiretaps.

[11] From 2000 to 2009, 78% of wiretap requests were reported in the year they occurred, and almost 19% were reported in the following year. The remaining 3% were reported in subsequent years.

I then aggregated these observations to the state-year level for analysis. Because I was interested in understanding the effects of the third-party doctrine on the frequency and intensity of intercept requests, I calculated the number of original requests for communication intercept orders in each state in each year and the number of overall requests for communication intercept orders (including both original requests and extensions) in each state in each year, as well as the total number of days that these requests authorized law enforcement to intercept communications in each state in each year. Where states did not report any intercept requests, each of these numbers was reported as zero. To account for variation in the size of each state, I divided both the number of intercept requests, number of overall intercept requests, and the days of interception authorized by the population of each state to calculate a rate. This resulted in 2,050 observations, each describing the rate of interception requests, rate of overall interception requests, and the rate of interception authorized per 100,000 people in a given state in a given year.

Summary statistics are presented below. As can be seen, a communication interception request is a relatively rare event, with a state using on average about 2 intercept requests per year and 81 authorized days of interception for every million people living in the state.[12] However, the standard deviation is greater than the mean for both the average number of intercept requests and days of interception, suggesting that there is a great deal of variation in intercept use across states. Comparing states that have and have not rejected the third party doctrine reveals that states that reject the third party doctrine use intercepts more intensively than states that do not reject the third party doctrine. Both the average number of intercept requests and the average days of interception are higher for states that reject the third party doctrine. Additionally, there is variation between intercept usage among states that have rejected the third party doctrine with respect to different types of information. The average number of intercept requests is highest among states that have rejected the third party doctrine with respect to phone records, while the average day of interception authorized is highest for states that have rejected the third party doctrine with respect to location information.

[12] Despite their relatively rare occurrence, communication intercepts remain a significant policy issue, particularly because each intercept request may result in many intercepted communications conducted by many different people, and a significant portion of these intercepted communications will be unrelated to any criminal activity. For example, 2264 intercept requests by state officials were reported in 2012, resulting in 7,126,193 intercepted communications involving up to 334,186 people; only 20.7% of the intercepted communications were incriminating.

Table 2.4. Summary Statistics for Data Describing Wiretap Usage

	Overall	*Third Party Doctrine Not Rejected*	*Third Party Doctrine Rejected*			
			Any	*Phone Records*	*Bank Records*	*Location Information*
Initial requests per 100,000 people	0.211 (0.514)	0.174 (0.463)	0.442 (0.718)	0.499 (0.725)	0.462 (0.643)	0.382 (0.833)
Overall requests per 100,000 people	0.315 (0.883)	0.260 (0.786)	0.660 (1.289)	0.690 (1.036)	0.627 (0.906)	0.720 (2.000)
Authorized days of interception per 100,000 people	8.135 (24.467)	6.691 (22.093)	17.150 (34.615)	17.492 (25.000)	17.291 (23.437)	20.902 (58.352)

This table describes state-level wiretap requests and authorizations from 1972-2012. The number of wiretap requests and authorized days of interception were obtained from the Wiretap Reports published by the Administrative Office of the U.S. Courts. These data were aggregated to the state-year level, resulting in 2,050 observations Overall summary statistics are provided, as well as summary statistics tabulated by whether and how the state supreme court had rejected the third party doctrine in a given state for a particular year. Mean and standard deviation (in parentheses) are provided.

3. Control Variables

The third party doctrine is not the only thing that could affect law enforcement intercept use. Because law enforcement uses communication intercepts in order to investigate serious crimes, intercept usage should be expected to change with changes in crime rates – particularly violent crimes and narcotics crimes. I control for urban drug sales arrests, urban gambling arrests, violent crime rate, and larceny rate through data obtained from the Uniform Crime Reports. Demographic and economic characteristics affect both crime rates and technology consumption practices, which may in turn influence the scope of third party data available to law enforcement. I therefore control for the percent of state population living in urban cities, percent male, percent white, and percent aged 20-34 using data obtained from the U.S. Census Bureau.

In addition, other aspects of state policies governing electronic surveillance could also affect law enforcement of electronic surveillance. I control for whether a state has a wiretap law in a given year using data obtained from the *Wiretap Reports*, as well as whether a state requires both parties to consent to the recording of a conversation, whether it is considered a violation of the state's Fourth Amendment equivalent when law enforcement records a conversation between a suspect and a cooperating, consenting informant, and whether the state supreme court has determined that their state constitutional Fourth Amendment equivalent is coextensive with the federal Fourth Amendment. I obtained information about two-party consent and informant consent by searching state supreme court jurisprudence through a procedure similar to the one described above. I obtained information about state supreme court decisions determining that their state constitutional protections are coextensive with the Federal Fourth Amendment by reviewing (Henderson 2006) and reviewing state supreme court jurisprudence.

Summary statistics for all control variables are described in Table 2.5 below.

Table 2.5. Summary Statistics for Control Variables

Group	*Control*	*Overall*	*Third Party Doctrine Not Rejected*	*Third Party Doctrine Rejected*			
				Any	*Phone Records*	*Bank Records*	*Location Info*
policy controls	two-party consent	0.200 (0.400)	0.168 (0.374)	0.399 (0.490)	0.376 (0.485)	0.276 (0.448)	0.500 (0.503)
	informant consent	0.123 (0.328)	0.112 (0.315)	0.194 (0.396)	0.219 (0.414)	0.319 (0.467)	0.045 (0.209)
	state wiretap law	0.697 (0.459)	0.661 (0.473)	0.922 (0.268)	0.919 (0.273)	0.907 (0.289)	1 0
	Fourth Amendment equivalent	0.085 (0.280)	0.099 (0.299)	0 0	0 0	0 0	0 0
urban arrest controls	urban drug sales arrests	645.267 (2466.518)	706.121 (2624.385)	217.874 (485.145)	239.162 (577.025)	162.960 (199.537)	158.645 (105.614)
	urban gambling arrests	79.971 (210.896)	86.494 (223.479)	34.158 (61.126)	25.837 (49.990)	40.707 (70.899)	40.410 (62.531)
crime controls	violent crime rate	432.710 (221.994)	427.132 (219.702)	467.540 (233.203)	488.081 (238.167)	541.063 (266.788)	387.277 (89.649)
	larceny rate	2647.213 (747.975)	2615.341 (709.639)	2846.217 (930.204)	2769.762 (901.440)	2784.455 (956.169)	2920.306 (789.259)
demo controls	percent urban	69.554 (14.670)	67.244 (14.085)	83.978 (8.889)	84.654 (9.153)	85.778 (7.392)	82.099 (4.768)
	percent male	0.490 (0.008)	0.490 (0.008)	0.493 (0.007)	0.494 (0.007)	0.493 (0.007)	0.496 (0.004)
	percent white	0.851 (0.122)	0.855 (0.110)	0.822 (0.180)	0.793 (0.198)	0.863 (0.059)	0.899 (0.048)
	percent young	0.228 (0.028)	0.229 (0.028)	0.223 (0.027)	0.219 (0.027)	0.228 (0.031)	0.218 (0.018)

Overall summary statistics are provided, as well as summary statistics tabulated by whether and how the state supreme court had rejected the third party doctrine in a given state for a particular year. All rates are per 100,000 people. Mean and standard deviation (in parentheses) are provided.

B. Analytic Strategy and Specification

1. Preliminary Analysis

In order to explore whether states that did and did not reject the third party doctrine used communication intercepts differently, I compared changes in law enforcement use of

communication intercepts before and after state supreme court opinions that addressed the third party doctrine, differentiating between states that decided to reject the third party doctrine, and those that did not.

2. Difference-in-Difference Analysis

I utilize a difference-in-difference methodology to analyze the effects of rejecting the third party doctrine on law enforcement use of communications intercepts. Difference-in-difference analyses are frequently used to determine the causal impact of laws because they allow comparison between states that have adopted the policies of interest and states that have not, and are robust to unobservable factors provided that those factors do not vary differently over time (Bertrand, Duflo, and Mullainathan 2002). Incorporating state and year fixed effects into this analysis enables further control for unobservable characteristics of state and global time trends. Standard errors were clustered by state.

First, I used difference-in-difference analysis to analyze the effects of rejection of the third party doctrine on the number of communication intercepts used, as specified in equations (I) and (II) below. I used a Poisson model to account for the count nature of the data. I conducted two separate analyses: one in which any state-level rejection of the third party doctrine was considered regardless of context, and one in which the specific types of investigative techniques accorded extra protection under state law were considered separately. Here, WT_{it} describes the number of communication intercepts per 100,000 people in state i in year t; $TPD_{ANY\,it}$ is a binary variable which is equal to 1 if state i has rejected the third-party doctrine in any circumstance in year t; and $TPD_{PR\,it}$, $TPD_{BR\,it}$, and $TPD_{LI\,it}$ are analogous variables describing rejection of the third-party doctrine in the context of phone records, bank records, and location information respectively. S_i is a set of state-level fixed effects, T_t is a set of year-level fixed effects, and X_{it} is a set of control variables describing the violent crime rate and the existence of state-level wiretap laws.

$$\ln(WT_{it}) = \beta_1 TPD_{ANY\,it} + \gamma S_i + \delta T_t + \gamma X_{it} + \epsilon_{it} \quad \text{(I)}$$

$$\ln(WT_{it}) = \beta_1 TPD_{PR\,it} + \beta_2 TPD_{BR\,it} + \beta_8 TPD_{LI\,it} + \gamma S_i + \delta T_t + \gamma X_{it} + \epsilon_{it} \quad \text{(II)}$$

In addition, I considered the effects of rejection of the third party doctrine on the number of overall requests for communication intercepts, including both initial intercept requests and requests for extensions, as specified in equations (III) and (IV) below. Here, OWT_{it} describes the total number of overall interception requests in each state in each year per 100,000 people.

$$\ln(OWT_{it}) = \beta_1 TPD_{ANY\,it} + \gamma S_i + \delta T_t + \gamma X_{it} + \epsilon_{it} \quad \text{(III)}$$

$$\ln(OWT_{it}) = \beta_1 TPD_{PR\,it} + \beta_2 TPD_{BR\,it} + \beta_8 TPD_{LI\,it} + \gamma S_i + \delta T_t + \gamma X_{it} + \epsilon_{it} \quad \text{(IV)}$$

Finally, I considered the effects of rejection of the third party doctrine on the total number of days of interception authorized in each state in each year, as specified in equations (V) and (VI) below. Here, DA_{it} describes the total days of interception authorized in each state in each year per 100,000 people.

$$\ln(DA_{it}) = \beta_1 TPD_{ANY\,it} + \gamma S_i + \delta T_t + \gamma X_{it} + \epsilon_{it} \quad \text{(V)}$$

$$\ln(DA_{it}) = \beta_1 TPD_{PR\,it} + \beta_2 TPD_{BR\,it} + \beta_8 TPD_{LI\,it} + \gamma S_i + \delta T_t + \gamma X_{it} + \epsilon_{it} \quad \text{(VI)}$$

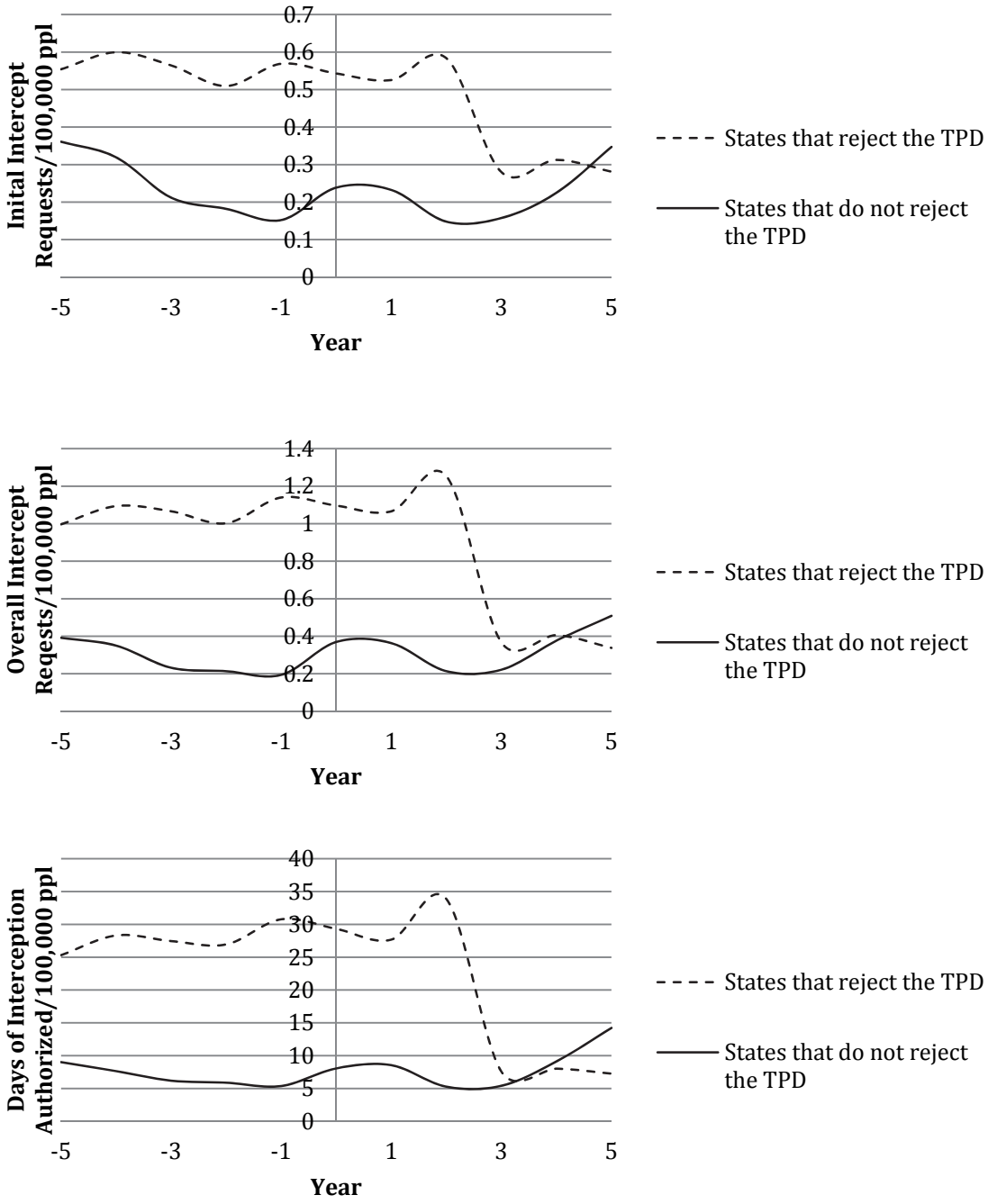
V. Results and Discussion

A. Preliminary Analysis

In order to explore how intercept use may be affected by increased protections for third party information, I examined intercept use immediately before and after state supreme court cases related to the third party doctrine. Using my coding of state supreme court cases, I was able to compare intercept use between states that reject the third party doctrine and those that consider, but do not reject, the third party doctrine. Because states that reject the third party doctrine and states that consider, but do not reject, the third party doctrine are arguably similarly situated before the release of the relevant state supreme court opinion, this analysis helps minimize endogeneity and therefore may be suggestive of causality. The results of this analysis are presented in Figure 2.5 below.[13]

[13] These graphs differentiate between states that do and do not reject the third party doctrine, without considering the type of information protected by the rejection of the third party doctrine. Similar graphs that take into consideration the type of information affected by the decision can be found in Appendix C.

Figure 2.5. Comparing Trends in Communications Intercepts



These charts describe trends in requests for communications intercepts by state-level law enforcement before and after state supreme court opinions related to the third party doctrine. Year 0 corresponds to the year in which the opinion was decided. Separate trend lines are presented for states that reject and do not reject third party doctrine with regards to any type of information.

As can be seen, prior to a judicial opinion related to the third party doctrine, it appears that states that reject the third party doctrine use more intercept requests than states that do not reject the third party doctrine. However, the trends in intercept use between states that reject the third party doctrine and do not reject the third party doctrine are roughly parallel. This suggests that the difference in intercept use between states that do and do not reject the third party doctrine is caused by characteristics of the state that do not change over time.

After the state supreme court decision is released, it appears that intercept use changes. However, this change is different in states that reject the third party doctrine and states that do not reject the third party doctrine. In states where the supreme court decision addressed – but did not reject – the third party doctrine, intercept use appears to remain the same or increase. However, in states where the supreme court decision rejected the third party doctrine, thereby increasing legal protections for third party information, all three measures of intercept use (rate of initial requests, rate of overall requests, and total days of interception authorized) appear to decrease. This decrease is delayed – generally occurring around the third year after the state supreme court decision is issued.

While these graphs suggest that rejecting the third party doctrine may cause decreased use of communications intercepts, there could be other factors underlying this apparent effect. Analyses that take into account additional state characteristics that might affect intercept use are needed to demonstrate causality.

B. Difference-in-Difference Analysis

Difference-in-difference analyses were used to provide causal evidence of the effect of rejecting the third party doctrine on law enforcement use of communications interceptions. Three different measures of intercept use were considered: the rate of initial intercept requests, the rate of overall intercept requests, and the rate of total days of interception authorized. In this section, I present the results from each analysis and discuss them in turn. I then conclude by discussing the implication of these results.

1. Effect of Rejecting the Third Party Doctrine on Initial Intercept Requests

Table 2.6 below presents the results of difference-in-difference analyses, exploring the effects of rejecting the third party doctrine on the rate of initial intercept requests.

Table 2.6. Effect of Rejecting the Third Party Doctrine on Rate of Initial Intercept Requests

	(I)	(I)	(I)	(II)	(II)	(II)
Any Rejection of TPD	-0.234	-0.436*	-0.315*			
	(0.255)	(0.246)	(0.162)			
Rejection of TPD for Phone Records				-0.159	-0.398*	-0.304
				(0.227)	(0.237)	(0.188)
Rejection of TPD for Bank Records				-0.151	-0.309	-0.045
				(0.207)	(0.223)	(0.149)
Rejection of TPD for Location Info				0.085	-0.272	-0.206
				(0.333)	(0.361)	(0.180)
Policy Controls	Y	Y	Y	Y	Y	Y
Urban Arrest Controls	N	Y	Y	N	Y	Y
Crime Controls	N	N	Y	N	N	Y
Demo Controls	N	N	Y	N	N	Y
Urbanicity Control	N	N	Y	N	N	Y
Year Fixed Effects	Y	Y	Y	Y	Y	Y
State Fixed Effects	Y	Y	Y	Y	Y	Y
N	1640	1383	1383	1640	1383	1383

This table provides the results of difference-in-difference analyses estimating the effects of rejecting the third party doctrine on the number of initial requests for communication intercepts made per 100,000 people in a given state in a given year. A Poisson regression model was used, and robust standard errors were used to account for clustering at the state level. State and year fixed effects were included on all regressions. *** denotes statistical significance at the 0.01 level; ** denotes statistical significance at the 0.05 level; *** denotes statistical significances at the 0.1 level.

When states increase protection for third party information by rejecting the third party doctrine, the rate of initial intercept requests decreases even when all control variables are incorporated into the model. This decrease is marginally statistically significant at the $\alpha=0.1$ level, although not statistically significant at the $\alpha=0.05$ level. The log of the expected rate of initial intercepts request decreases by -0.315 when a state rejects the third party doctrine, corresponding to a decrease in the expected rate of initial intercept requests by a factor of 0.729.

If the analysis differentiates between the types of information affected by state supreme court rejection of the third party doctrine, then increasing protection for third party information does not affect the rate of initial intercept requests. While there is a marginally significant

relationship between legal protections for phone records and the rate of initial wiretap requests, this relationship is not observed when all control variables are incorporated into the model. Regardless of the use of control variables, increasing protection for bank records and location information does not appear to have an observable effect on the rate of initial intercept requests.

2. Effect of Rejecting the Third Party Doctrine on Overall Intercept Requests

Table 2.7 below presents the results of difference-in-difference analyses, exploring the effects of rejecting the third party doctrine on the rate of overall intercept requests.

Table 2.7. Effect of Rejecting the Third Party Doctrine on Rate of Overall Intercept Requests

	(III)	(III)	(III)	(IV)	(IV)	(IV)
Any Rejection of TPD	-0.274	-0.431**	-0.306**			
	(0.210)	(0.202)	(0.142)			
Rejection of TPD for Phone Records				-0.405	-0.624**	-0.476**
				(0.271)	(0.273)	(0.194)
Rejection of TPD for Bank Records				-0.195	-0.338*	-0.162
				(0.197)	(0.200)	(0.150)
Rejection of TPD for Location Info				0.117	-0.068	-0.043
				(0.268)	(0.325)	(0.190)
Policy Controls	Y	Y	Y	Y	Y	Y
Urban Arrest Controls	N	Y	Y	N	Y	Y
Crime Controls	N	N	Y	N	N	Y
Demo Controls	N	N	Y	N	N	Y
Urbanicity Control	N	N	Y	N	N	Y
Year Fixed Effects	Y	Y	Y	Y	Y	Y
State Fixed Effects	Y	Y	Y	Y	Y	Y
N	1640	1383	1383	1640	1383	1383

This table provides the results of difference-in-difference analyses estimating the effects of rejecting the third party doctrine on the overall number of requests for communication intercepts made per 100,000 people in a given state in a given year. A Poisson regression model was used, and robust standard errors were used to account for clustering at the state level. State and year fixed effects were included on all regressions. *** denotes statistical significance at the 0.01 level; ** denotes statistical significance at the 0.05 level; *** denotes statistical significances at the 0.1 level.

The rate of overall interception requests decreases when states increase protection for third party information by rejecting the third party doctrine. This decrease is statistically significant at the $\alpha=0.05$ level as long as urban narcotics and gambling arrests are controlled for in the model, which is unsurprising given that communications intercepts primarily originated as a method for

investigating these crimes. After all controls are included in the model, the log of the expected rate of overall intercept requests decreases by -0.306 when a state rejects the third party doctrine, corresponding to a decrease in the expected rate of overall intercept requests by a factor of 0.736.

After differentiating between the types of information protected by state supreme court rejection of the third party doctrine, providing additional protections to phone records is associated with a statistically significant decrease in the rate of overall intercept requests. After incorporating all control variables in the model, providing additional protections by rejecting the third party doctrine with respect to phone records is associated with a change of -0.476 in the log of the expected rate of overall intercept requests, corresponding to a decrease in the expected rate of overall intercept requests by a factor of 0.621. In addition, providing additional protections for bank records has a marginal, negative effect on the rate of overall interception requests, which disappears once all control variables are incorporated into the model.

3. Effect of Rejecting the Third Party Doctrine on Days of Interception Authorized

Table 2.8 below presents the results of a series of difference-in-difference analyses, exploring the effects of rejecting the third party doctrine on the rate of days of interception authorized.

Table 2.8. Effect of Rejecting the Third Party Doctrine on the Rate of Days of Interception Authorized

	(V)	(V)	(V)	(VI)	(VI)	(VI)
Any Rejection of TPD	-0.396*	-0.540**	-0.353**			
	(0.215)	(0.214)	(0.142)			
Rejection of TPD for Phone Records				-0.506*	-0.756***	-0.547***
				(0.269)	(0.265)	(0.187)
Rejection of TPD for Bank Records				-0.246	-0.412**	-0.160
				(0.198)	(0.186)	(0.135)
Rejection of TPD for Location Info				-0.027	-0.212	-0.108
				(0.268)	(0.307)	(0.181)
Policy Controls	Y	Y	Y	Y	Y	Y
Urban Arrest Controls	N	Y	Y	N	Y	Y
Crime Controls	N	N	Y	N	N	Y
Demo Controls	N	N	Y	N	N	Y
Urbanicity Control	N	N	Y	N	N	Y
Year Fixed Effects	Y	Y	Y	Y	Y	Y
State Fixed Effects	Y	Y	Y	Y	Y	Y
N	1640	1383	1383	1640	1383	1383

This table provides the results of difference-in-difference analyses estimating the effects of rejecting the third party doctrine on the total number of days of interception authorized per 100,000 people in a given state in a given year. A Poisson regression model was used, and robust standard errors were used to account for clustering at the state level. State and year fixed effects were included on all regressions. *** denotes statistical significance at the 0.01 level; ** denotes statistical significance at the 0.05 level; *** denotes statistical significances at the 0.1 level.

The rate of total days of interception authorized decreases when state supreme courts provide additional protections for commercial information by rejecting the third party doctrine. This decrease is statistically significant at the α=0.05 level. After including all controls in the model, the log of the estimated number of days of interception authorized changes by -0.353 when a state rejects the third party doctrine, corresponding to a decrease in the estimated number of days of interception per 100,000 people by a factor of 0.702.

If the specific type of information protected by the rejection of the third party doctrine is considered, then additional protections to phone records decreases the estimated number of days of interception authorized. Rejection of the third party doctrine with respect to phone records is associated with a change of -0.547 in the log of the estimated rate of days of interception

authorized, corresponding to a decrease in the estimated rate of days of interception authorized by a factor of 0.578.

4. Implications for Law Enforcement Decision Making

When state supreme courts provide additional protections for third party information by rejecting the third party doctrine, it appears that law enforcement uses fewer communications intercepts to investigate crimes. This suggests that these two forms of surveillance may act as complements. While this reduction is only marginally significant for the rate of initial requests for communication intercepts, it is fully significant for the rate of overall intercept requests and the rate of total days of interception authorized. When the types of information protected by the state supreme court's rejection of the third party doctrine are considered separately, a similar pattern emerges for phone records. Additional legal protections for phone records do not appear to affect the rate of initial requests for communications intercepts, but do affect the rate of overall number of communications requests and the rate of total days of interception authorized. Additional legal protections for bank records and location information appear to have no effect on law enforcement use of communications intercepts.

Based on these results, it could be argued that additional protections for third party information may reduce law enforcement use of communications intercepts on the intensive, but not extensive, margins. The number of initial requests of communication intercepts may be an appropriate, although not precise,[14] proxy for the number of investigations in which communication intercepts are used. Under this assumption, rejection of the third party doctrine appears to have little to no effect on the number of investigations that use communications intercepts. The extent of law enforcement use of communications intercepts remains unchanged.

However, even though the number of initial intercept requests is unaffected by rejection of the third party doctrine, it appears that additional protections for third party information may reduce the length of time an intercept is used. Both the overall number of requests (encompassing initial requests for intercept authorization and requests to extend this authorization) and the number of days of interception authorized decrease after a state rejects the third party doctrine. Even if law enforcement does not use communications intercepts less often after the third party doctrine is rejected, it appears that they use each intercept for a shorter length of time.

These results suggest that rejection of the third party doctrine may cause law enforcement to delay use of communications intercepts during an investigation. Third party information –

[14] Multiple interception requests may be used in the same investigation, and the *Wiretap Reports* will sometimes include information on whether an intercept request was related to a different intercept request. However, as this information is not reported consistently over the timespan in question, it may not be possible to accurately relate the number of interceptions to the number of investigations in which an interception was used. However, this may be an appropriate estimation for a first approximation.

particularly phone records requests – provides crucial evidence in support of an application for an authorized communication interception. When a state rejects the third party doctrine, law enforcement officers must meet a higher standard before they can use third party information. To meet this standard, law enforcement must now develop their case further before using third party information, and consequently before using communications intercepts. As the case is further developed before use of the communication intercept begins, law enforcement does not need to gather as much information from the communication intercept and therefore uses it for a shorter period of time, resulting in fewer overall wiretap requests and fewer days of interception authorized.

Law enforcement use of communication intercepts appears to be affected by legal protections for phone records requests, but not legal protections for bank records or location information. This may be explained by the close connection between phone records and the evidence required for authorization for a communications intercept. To obtain judicial permission to use a communications intercept, law enforcement must demonstrate that the phone in question has been used or is likely to be used in the commission of a criminal act. Phone records – which can reveal who the phone has been used to call – provide uniquely relevant information demonstrating that the phone has been used for criminal purposes. Consequently, it is logical that making it more difficult for law enforcement to obtain phone records may decrease law enforcement use of communications intercepts. Such an effect may not be seen for bank records because the information they provide is not as closely related to communications, and equivalent information may be obtained through other sources.

The results obtained from the difference-in-difference analysis are supported by the results of the preliminary graphical analysis: both demonstrate that rejection of the third party doctrine decreases law enforcement use of communications intercepts. However, the graphical analysis implies that there may be a delay between the rejection of the third party doctrine and the decrease in communications intercepts. This delay suggests that additional legal protections for third party data may not have an effect on criminal investigations currently underway. Since communications intercepts are usually used in complex organized crime or narcotics cases, it is plausible that it could be several years before new cases are developed enough for the investigating officers to consider the use of communications intercepts.

C. Sensitivity Analysis

There are a variety of assumptions underlying this analysis. First, I consider only state supreme court decisions related to the third party doctrine, ignoring the fact states could enact similar protections legislatively. Additionally, states that reject the third party doctrine could be different in some unobservable way from states that do not reject the third party doctrine. For example, privacy advocates in some states may undertake a campaign to reduce law enforcement surveillance, yielding both lawsuits that lead to rejection of the third party doctrine and decreased use of wiretaps due to political pressure. Therefore, I test the sensitivity of my results

in two ways. First, I first recoded the variables describing whether and how state supreme courts had protected third party information by rejecting the third party doctrine to include passage of state statutory laws providing analogous protections. Second, I repeated my analysis, omitting all states where there had never been a state supreme court case addressing the third party doctrine. Because there could arguably be unobservable differences between states that address the third party doctrine and states that do not address the third party doctrine, this analysis helps minimize endogenous factors that could be driving my results. Tables describing the results of both these analyses are provided in Appendix D.

Including state statutory provisions that provided similar protections for third party information yielded similar, but not, identical results. In my main analysis, the effect of protecting third party information on the rate of initial intercept requests was marginally significant when considering rejection of the third party doctrine for any type of information; in this sensitivity analysis, it is no longer statistically significant. However, the effect of providing protection for third party information on the rate of overall intercept requests and the rate of total days of interception authorized is statistically significant and has a similar effect size in both analyses. When the type of third party information protected is considered, the main analyses and sensitivity analyses are again similar in both significance and effect size.

Omitting all states where the state supreme court never considered the third party doctrine yielded results that were similar in some ways and different in others. When the analysis only considered whether the state had rejected the third party doctrine, and did not account for the type of information protected by these rejection, rejection of the third party doctrine no longer had a statistically significant effect on the rate of initial interception requests, overall interception requests, or the days of interception authorized. It is possible that this loss of statistical significance may be due in part to the substantially decreased number of observations: while there were 1383 observations in the main analyses, there were only 672 observations after omitting all states that had never considered the third party doctrine. However, when the analyses accounted for the type of information protected by rejection of the third party doctrine, it appeared that rejection of the third party doctrine with respect to phone records had a statistically significant and negative effect on both the rate of overall requests and the total days of interception authorized – as found in my main analyses.

D. Limitations

First, this analysis is limited in scope. It provides evidence suggesting a relationship between two specific types of investigative techniques: third party data requests and communications intercepts. Law enforcement uses many other forms of investigative techniques, and use of these techniques may be related in interesting and important ways. However, further research is needed in order to understand how the apparent connection between law enforcement access to third party data requests and use of communications intercepts fits into a larger understanding of how law enforcement officers conduct investigations.

Additionally, this analysis is based largely on administrative data obtained from the *Wiretap Reports* published by the Administrative Office of the U.S. Courts. If these data are not accurate, then my results may be compromised. There are several reasons to believe that my analysis will be minimally affected by inaccuracies in reporting. First, federal law requires judges to report any requests for communications intercepts they receive, and prosecutors involved with these requests to report outcomes associated with each intercept request granted. Second, for purposes of this data I draw only from the information provided by judges who receive requests for communication intercepts. This may reduce the inaccuracy of my data because judges have no incentive to conceal or delay reports of electronic surveillance. Finally, because I use a difference-in-difference analysis, my results should be robust to errors in reporting, assuming that these errors do not change differentially over time. For example, my results will be unaffected if reporting of communications intercepts has become universally more accurate over time as judges become increasingly aware of the importance of transparency.

Furthermore, this analysis assumed that all instances where a state supreme court rejects the third party doctrine with regards to a particular type of information will have the same effect on law enforcement use of communications intercepts. Particularly in the instance of location information, this may be an uncertain assumption. Technology behind electronic location tracking has improved greatly in the 40 years included in this analysis, and the GPS devices regulated by later state supreme court cases are capable of providing much more detailed information then the transmitting beepers regulated by earlier cases. It may be that, while regulating GPS trackers has an effect on law enforcement use of communication intercepts, these effects are obscured in the analysis by grouping them in with technology that provides less specific information. Further analyses that account for policy heterogeneity, perhaps by using synthetic control groups, may provide different results.

Also, this research only considers the actions of state law enforcement, ignoring the potential for cooperation between officers at the federal and state levels. Rejection of the third party doctrine by a state supreme court would make it more difficult for state law enforcement officers to obtain third party information, but would not apply to any federal officer investigating federal crimes within that state. Therefore, a state-level officer who saw his case stymied by strict state privacy laws could elect to pass the case on to a federal officer operating in his jurisdiction, assuming that the activity in question could constitute a federal offense and the federal officer was willing to take the case. Further research is needed to explore the interactions between use of electronic surveillance by state law enforcement and federal law enforcement.

Finally, this analysis only considers how rejection of the third party doctrine affects law enforcement use of communications intercepts along three specific dimensions: the number of initial intercept requests, the number of overall intercept requests, and the total number of days of interception authorized. However, rejection of the third party doctrine could change law enforcement use of communications intercepts in many other ways. For example, rejecting the third party doctrine could increase the efficiency of communications intercepts, since law

enforcement has further developed their case before requesting an intercept. Costs could be lower, since the intercept is used for a shorter length of time and law enforcement may be able to select more productive targets. However, the savings could be offset by increased costs at the beginning of the investigation, as law enforcement must now gather additional evidence before requesting access to phone records. Further analysis is needed in order to fully understand the impact of rejecting the third party doctrine on how law enforcement uses surveillance.

VI. Conclusions and Policy Implications

Fourth Amendment jurisprudence has been described as seeking "a balance of police power" which "give[s] government officials some powers to enforce the law and yet also restrict[s] that power to avoid government abuses" (Kerr 2011, p. 485). This research suggests two sources of complexity that should be considered when attempting to maintain this balance of power. First, restricting law enforcement access to certain surveillance tools may have downstream effects on their ability to use other types of surveillance. Second, the effect of changes in privacy law on law enforcement surveillance may be difficult to describe as a simple "increase" or "decrease." For example, rejection of the third party doctrine appears to have shortened the length of intercept use, but not reduced the number of initial intercepts requested.

Based on this research, policymakers and advocates who are concerned that law enforcement efficacy may suffer if privacy rights are expanded should consider the relationship between different forms of surveillance when regulating law enforcement investigations. They may want to argue that policies regulating law enforcement access to third party data should account for how these restrictions could affect use of other forms of surveillance. Public safety oriented policymakers may therefore want to advocate for comprehensive electronic surveillance reform, which would allow legislators to consider not just how each form of surveillance should be regulated individually, but also craft regulations that address electronic surveillance as a system in order to minimize unintended consequences.

However, for privacy advocates this work could instead demonstrate the unintended benefits of protecting privacy rights. As this research suggests that restricting phone records requests seems to reduce reliance on communications intercepts, privacy advocates may want to argue that improving protections for third party information will protect privacy in unexpected ways. In the particular instance of legal protections for phone records and communications, it appears that protecting one type of information (phone records) can increase protection for another type of information (communications) without requiring additional regulation or policymaking. However, the relationship between different privacy protections may not always function in this way. For example, it is conceivable that increasing privacy protections for phone records could increase law enforcement use of location information, as law enforcement officers may now be more likely to use location information to demonstrate that two people communicate with each other by showing they are frequently in the same place. By considering how different types of

privacy rights can interact in positive and negative ways, privacy protections can be more carefully crafted to maximize positive side effects and minimize negative side effects.

3. Reconsidering Law Enforcement Use of Technological Search and Seizure: Dollars and Sense[15]

Abstract

Recent technological innovations have profoundly changed the way that law enforcement officers gather information about criminal activities. Not only does law enforcement have new tools for conducting electronic surveillance, but they can also take advantage of data collected by commercial entities. Both of these developments have reduced what have been referred to as "structural privacy rights": privacy interests that arise not from law, but from the financial and technical difficulties in data collection. However, as very little is currently known about how law enforcement decides to use electronic surveillance, it is difficult to understand how legal and structural privacy rights actually affect this decision making process. Without a clearer picture of how law enforcement decides to use electronic surveillance, policy interventions in this area may lead to unintended consequences. Furthermore, as commercial data collection has become nearly ubiquitous, the use of this information in criminal investigations has also risen. Unless more is known about whether and how law enforcement uses these two types of techniques differently, it will be difficult to craft policies that accurately account for practical obstacles faced by the officers who use them.

In this paper, I attempt to fill this gap by exploring how law enforcement officers decide to use electronic surveillance and commercial information requests. To do this, I conducted semi-structured interviews with 23 law enforcement officers who use electronic surveillance regularly. My interviews revealed five factors that law enforcement considered when deciding to use electronic surveillance or commercial information requests: legal concerns, resource concerns, safety concerns, investigatory concerns, and information concerns. While the first two categories relate to the legal and resource constraints frequently identified as regulating law enforcement use of surveillance, the last three reveal new factors that affect this decision making process. Additionally, the law enforcement officers interviewed identified different factors when discussing electronic surveillance use versus commercial information requests. While investigatory concerns were frequently cited for both electronic surveillance and commercial information requests, resource concerns were cited much more often for electronic surveillance and information concerns were cited much more often for commercial information requests.

[15] This work was funded by the James Q. Wilson Dissertation Fellowship at the Pardee RAND Graduate School. I would like to thank my Ed Balkovich, Sasha Romanosky, James Anderson, and Derek Bambauer for their valuable comments and feedback. I would also like to thank participants from the 2016 Law and Society Association Annual Meeting for their helpful questions and suggestions.

I. Introduction and Background

Recent technological innovations have profoundly changed the way law enforcement officers conduct investigations. New electronic surveillance techniques have been developed, enabling law enforcement to collect detailed information about criminal suspects effectively and efficiently. Perhaps more significantly, law enforcement agencies are no longer the only entities conducting electronic surveillance. Commercial entities – particularly the developers and manufacturers of consumer devices – now collect, store, share, and analyze tremendous amounts of data about their customers. By requesting customer data from commercial entities, law enforcement may be able to obtain information that they could not otherwise access without expending time and resources on electronic surveillance.[28] In some circumstances, the information obtained through commercial information requests can be strikingly similar to information obtained through electronic surveillance. For example, law enforcement can obtain information about a suspect's location by placing a GPS tracker on their car (*U.S. v. Jones*, 565 U.S. 945 (2012)) or requesting cell site information from a phone company (*U.S. v. Graham*, 2016 U.S. App. LEXIS 9797 (4th Cir. 2016)).

Technological innovations, including improvements in both electronic surveillance and commercial collection of information, can be powerful tools for improving criminal investigations and promoting safe communities (Nunn 2008). However, both policymakers and the general public have expressed deep concern that advances in government exploitation of technology may undermine the traditional balance between public safety and individual privacy enshrined in the Fourth Amendment (Frenkel 2013). In particular, some have argued that the staggering increase in the breadth and depth of commercially-collected data available to law enforcement "poses significant problems with far-reaching social effects" (Solove 2002).

Many have argued that improved surveillance technologies have reduced the implicit privacy protections created by the difficulty of obtaining information (Selinger and Hartzog 2014). For example, law enforcement once had to physically review a person's letters in order to determine whether they referenced criminal activity. Similar information can now be obtained quickly and cheaply by performing a key word search on digital documents, greatly reducing the costs of conducting the search and increasing the ease of obtaining this information (Surden 2007). Also known as structural privacy

[28] As will be later discussed, under an element of Fourth Amendment jurisprudence known as the third party doctrine, individuals do not enjoy protection in information they have shared with third parties, including commercial services providers. *See Smith v. Maryland*, 442 U.S. 735 (1979).

rights,[29] these practical restrictions on information collection have long been an important source of privacy protections. There is currently much public debate about the extent to which improved surveillance technologies have undermined structural privacy rights, and whether legal protections should be extended in order to compensate for lost structural privacy rights.

There are many unanswered questions about how law enforcement uses electronic surveillance and commercial information requests that would inform this debate. Little research has been conducted on how law enforcement decides to use electronic surveillance and commercial information requests. A clear description of what law enforcement officers consider when deciding to use electronic surveillance could yield not only a description of how legal and resource restraints affect surveillance use, but also identify other factors that contribute to this decision. It may also identify differences between how law enforcement uses electronic surveillance and commercial information requests. While law enforcement may be able to use these techniques in similar situations to achieve similar goals, the laws governing use of these techniques are very different. A clearer description of whether and how use of these techniques differs could help policymakers determine whether they should continue to be regulated differently.

Additionally, by describing the decision to use electronic surveillance and commercial information requests, it may be possible to identify and understand barriers to use of these techniques. Identifying these barriers may help lawmakers craft policies that provide effective oversight of law enforcement while minimizing unintended consequences. A description of how law enforcement uses electronic surveillance and commercial information requests could also help determine the extent to which traditional structural privacy rights have failed, and spot new sources of structural privacy rights.

In this paper, I attempt to answer these unanswered questions by exploring how law enforcement uses electronic surveillance and commercial information requests. Specifically, I seek to answer two questions: (1) What does law enforcement consider when deciding to use electronic surveillance and commercial information requests? (2) How do the factors law enforcement consider when deciding to use electronic surveillance and commercial information requests differ?

To answer these questions, I conducted semi-structured interviews with 23 law enforcement officers who use electronic surveillance regularly. During these interviews, I asked the officers to recall a recent investigation in which they used electronic surveillance, and then describe how they decided to use electronic surveillance in that

[29] According to Surden (2007), structural privacy rights are defined as privacy interests protected by "the secondary costs arising from the current technological state of the world." (Surden 2007, 1613).

case. I then repeated this process with a recent investigation in which they used commercial information requests. The results of these interviews were carefully analyzed and coded for themes in order to identify a list of concerns that law enforcement considered when deciding to use electronic surveillance.

My interviews revealed five factors that law enforcement considered when deciding to use electronic surveillance: legal concerns, resource concerns, safety concerns, investigatory concerns, and information concerns. While the first two categories relate to the legal and resource constraints frequently identified as regulating law enforcement use of surveillance, the last three reveal new factors that affect this decision making process. I discuss the implication of my results for several important policy issues related to electronic surveillance. In particular, I describe the barriers to law enforcement use of electronic surveillance and commercial information requests, discuss the extent to which cost continues to play a role in the electronic surveillance decision-making process, and identify potential new structural privacy protections in this domain. I conclude by discussing the policy implications of my work. In particular, I describe new barriers that may affect law enforcement use of electronic surveillance and commercial information requests, and discuss the evolving role of commercial entities in regulating law enforcement surveillance.

A. Defining Electronic Surveillance and Commercial Information Requests

Technological advances have radically transformed the way that law enforcement collects information about suspects. Electronic surveillance has become a key component of the law enforcement officer's toolbox; however, there are some disagreements over which specific techniques should be included within this term. Most definitions of electronic surveillance are crafted for limited circumstances, and may not be broad enough to capture many things that would commonly be thought of as electronic surveillance. For example, the Foreign Intelligence Surveillance Act (FISA) defines electronic surveillance as "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication" under various circumstances, as well as the "installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy" (50 U.S.C. §1801(f)). While this definition may be well suited for particular legal arguments, it does not correspond to the meaning of electronic surveillance as commonly understood by law enforcement officers.

For purposes of this paper, I adopt a definition of electronic surveillance based on how this term may be commonly understood by law enforcement – and, indeed, based on how the law enforcement officers I talked to defined this term. Such a term includes a

broad variety of techniques, including such things as use of GPS trackers, communications intercepts, cell phone tracking, surveillance cameras, body wires, and drones. Consequently, the key distinction I make is not between different forms of electronic surveillance, but between whether the entity using electronic means to collect information is law enforcement or a commercial entity. Electronic surveillance is defined as a technique where law enforcement uses technological means to collect information; in contrast, I use the term "commercial information request to refer to situations where law enforcement requests information that was first collected by a commercial entity. The one exception to this rule is use of cell phone location tracking, which I define as a form of electronic surveillance, following the lead of the majority of my respondents.[30] This approach runs the risk of devolving into a Stewart-esque tautology,[31] where we do not define electronic surveillance, but rather "know it when we see it." However, because the goal of this paper is to describe electronic surveillance decision making from the perspective of law enforcement officers, it was important to adopt a definition of electronic surveillance that tracked with their understanding of the term.

The term "commercial information requests" therefore incorporates a variety of different types of information that are collected by commercial entities and subsequently requested by law enforcement for use in criminal investigations. Examples of information types that might be requested by law enforcement include phone records, bank records, records from internet service providers, and records from social networking websites. While it may seem that these records cannot reveal much about an individual, they may actually provide incredibly detailed (and intimate) information that can be vital to law enforcement investigations. For example, a recent study analyzed a dataset consisting of telephone metadata voluntarily contributed by over 800 participants. Researchers found that they could describe an individual's communication patterns in a way that would support inferences about their health conditions, reproductive decision-making, illegal drug use, and gun ownership (Mayer et al. 2016).

B. Legal Protections Against Government Surveillance

The primary source of protections for individuals targeted by law enforcement searches, the Fourth Amendment protects "persons, houses, papers and effects" against

---

[30] The fact that many of the law enforcement officers I interviewed listed cell phone location tracking as an example of electronic surveillance points to the conceptual difficulties of this area. It also suggests a convergence between law enforcement initiated surveillance and law enforcement use of commercially initially surveillance, as the commercially initiated surveillance begins to yield sufficiently detailed information.

[31] Justice Stewart famously remarked that, while "perhaps [he] could never succeed in intelligibly" defining obscenity, he "know[s] it when [he] see[s] it." *Jacobellis v. Ohio*, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).

"unreasonable searches and seizures" by the government (U.S. Const. Amend. IV.).[32] Although the text of the amendment does not reference privacy, Supreme Court jurisprudence has made protection by the Fourth Amendment contingent on societally understood privacy interests. As most famously articulated by Justice Harlan's concurring opinion in *Katz v. United States*, there is a "twofold requirement" for Fourth Amendment protections to be triggered: "first, that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'" (*Katz v. United States*, 389 U.S. 347 (1967)). While there is no clear formula for determining whether law enforcement conduct has violated a reasonable expectation of privacy, courts often look to whether the conduct impacted a place that traditionally enjoyed Constitutional protection and the type of information sought (Kerr 2007), as well as "whether the government's intrusion infringes upon the personal and society values protected by the Fourth Amendment" (*Oliver v. United States*, 466 U.S. 170, 182-3 (1984)).

Although *Katz v. United States* made it clear that "the Fourth Amendment protects people, not places" (*Katz v. United States*, 389 U.S. at 351), an individual's reasonable expectation of privacy often tracks property rights (Kerr 2004). As "the very core" of the Fourth Amendment includes "the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion," courts often find that a search has occurred where technology has allowed law enforcement to obtain information from within a home[33] or other private space (*Florida v. Jardines*, 569 U.S. 1 (2013)). For example, use of a thermal imaging device to obtain information about the heat emanating from a house constitutes a search because it involves a sense-enhancing technology not generally used by the public being employed to gather "information regarding the interior of the home that could not otherwise have been obtained without" physically entering the house (*Kyllo v. United States*, 533 U.S. 27, 35 (2000)). In contrast, courts generally hold that law enforcement observation of activities and communications conducted in public is not considered a search for purposes of the Fourth Amendment, even when technology is used to assist this observation. For example, the Supreme Court has held that law

[32] Although the Fourth Amendment is a fundamental source of rights for individuals targeted by law enforcement surveillance, some have argued that statutory law could and should play an important role in protecting privacy in the context of the Fourth Amendment. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801 (2004).

[33] Fourth Amendment protections related to the home are generally applied not only to the building's interior, but also to the building's "curtilage" – the area immediately surrounding the home that "harbors the intimate activity associated with the sanctity of a man's home and the privacies of life" (*United States v. Dunn*, 480 U.S. 294 (1987) *(internal quotations omitted)*).

enforcement use of a beeper to track a drum of chemicals on public roadways did not constitute a search for purposes of the Fourth Amendment, because "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another" (*United States v. Knotts*, 460 U.S. 276, 281 (1983)).[34]

However, these Fourth Amendment protections do not apply to all circumstances where law enforcement is collecting information about a suspect. Under what is known as the third party doctrine, the government can obtain information that an individual has shared with a third party without implicating that individual's Fourth Amendment rights (*Smith v. Maryland*, 442 U.S. 735 (1979)). Because information can no longer be considered private once it has been shared, an individual "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government" (*United States v. Miller*, 425 U.S. 435, 442 (1976)). As the third party doctrine applies to information an individual has shared with commercial entities, the increase in consumer data collection has meant that there is an increase in the amount of information law enforcement can access without a warrant (Spencer 2013).

In addition to federal Constitutional protections, every state constitution includes an amendment that provides analogous – and sometimes greater – protection to individual rights. Indeed, state constitutions have been described as "a font of individual liberties, their protections often extending beyond those required by the Supreme Court's interpretation of federal law" (Brennan 1977, 491). For example, although the federal Constitution does not require law enforcement to obtain a warrant before seeking information that an individual has shared with a third party, several state supreme courts

---

[34] In this particular case, there was no indication that law enforcement used the beeper to obtain information about the automobile after it had arrived on the defendant's private property (*United States v. Knotts*, 460 U.S. 276, 284-285 (1983)). Subsequent case law has held that monitoring a tracking beeper while the object containing the beeper is within a home does constitute a search for purposes of the Fourth Amendment (*United States v. Karo*, 468 U.S. 705 (1984)). The particular technology used in these cases – radio-based tracking beepers – provides relatively unsophisticated location information. However, law enforcement can now track location using sophisticated GPS devices, which can provide very detailed information about an individual's location. In *United States v. Jones* (2012), the Supreme Court was presented with the issue of whether law enforcement use of GPS tracking devices is a Fourth Amendment search. The majority of the Supreme Court held that a search had occurred based on attachment of the GPS tracker to the defendant's car (and consequently did not reach the issue of whether use of the tracker constitutes a search). Four concurring justices would have instead determined whether a Fourth Amendment search occurred by asking whether use of the GPS tracker in this particular instance "involved a degree of intrusion that a reasonable person would not have anticipated" (*Id.* at 964).

interpreted their state constitutions as requiring a warrant before law enforcement can collect certain types of third party information (Henderson 2006).

Legislators on both the federal and state level have also been active in crafting protections to the subjects of criminal investigations. For example, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which established many of the procedures that law enforcement must comply with to obtain a wiretap. Several states have recently adopted regulations on law enforcement use of location information. According to the American Civil Liberties Union, as of June 2014 thirteen states had adopted laws pertaining to the use of location information by law enforcement, and an additional nine had considered adopting such laws. (Bohm 2014). For example, Colorado requires law enforcement to obtain a warrant before accessing location information generated by a mobile device, while Montana requires that law enforcement obtain a warrant before they access information created by "a global positioning service or other mapping, locational, or directional information service" (Col. Rev. Stat. sec. 16-3-303.5; Mont. Code Ann. sec. 46-5-110).

C. Practical Protections Against Government Surveillance

Legal rights have never been the only – or even the primary – source of privacy protections in the United States. As Justice Alito wrote, "[i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical" (*United States v. Jones*, 132 S. Ct. 945, 963 (2012)). Surden (2007) describes these practical protections for privacy as "structural rights": mechanisms which "impose physical or technological costs on behaviors" that infringe on privacy interests, thus reducing the behaviors and increasing privacy (Surden 2007, 1610).

Structural privacy rights may falter when changes in technology reduce or eliminate existing barriers to obtaining information (Bankston and Soltani 2014). In that case, some scholars have suggested that courts should – and do – step in to expand legal protections when technological innovations make it easier for law enforcement officers to obtain information about individuals. Because "Fourth Amendment rules are under constant attack from technological change and morphing social practices", courts adjust their interpretation of the Fourth Amendment to provide constant limits on law enforcement over time (Kerr 2011).

However, it is not clear the extent to which structural privacy protections have been undermined by the adoption of electronic surveillance. While it may sometimes be less expensive than traditional investigative techniques, electronic surveillance can still be costly. Additionally, many types of electronic surveillance may require infrastructure, specialized devices, and technical knowledge. Without these assets, law enforcement may be limited in the type or scope of electronic surveillance they can undertake. Furthermore, since technological devices may share information in unexpected ways, law

enforcement may be unaware of the surveillance options available to them. Although these structural protections may have shifted as technological improvements increase the availability of information, there are still very real practical limitations on law enforcement's ability to conduct electronic surveillance. In the remainder of this section, I describe two of these limitations: cost/manpower requirements and technological capabilities/capacities.

1. Cost and Manpower Requirements

Like any other actor, law enforcement agencies are subject to budget and other resource constraints. The cost of conducting electronic surveillance varies greatly depending on the techniques used. Forms of electronic surveillance that require the active participation of law enforcement, such as wiretaps, pen registers, trap and trace devices, and stingray devices,[35] can be extraordinarily expensive. Forms of electronic surveillance that rely on law enforcement gaining access to records generated by commercial entities such as use of metadata and historical cell site information, may cost significantly less.

Forms of electronic surveillance that rely on the active participation of law enforcement can require both expensive equipment and extensive manpower. According to the most recent Wiretap Report,[36] an average intercept order cost $41,119 in 2013; however, this cost may extend into "hundreds of thousands of dollars" for a single case (Strange 2015). A large part of this cost is due to the manpower required to execute communications intercepts: since wiretaps are subject to a minimization requirement, a trained and knowledgeable agent must be available to listen to the beginning of a particular conversation and determine whether the call should be monitored and recorded. Additionally, law enforcement agencies are required to reimburse telecommunications providers "for reasonable expenses incurred in providing such facilities or assistance." (18 U.S.C. § 2518(d)). Pen registers can be similarly expensive; according to one Texas prosecutor, "[a] police agency wishing to use [pen registers] will invest between $20,000 and $30,000 in equipment and specialized training" (Strange 2015).

However, forms of electronic surveillance that rely on data collected by commercial entities can have substantially lower costs. Bankston and Soltani (2014) estimated the

---

[35] A stingray device is an apparatus that mimics a cellular tower in order to identify cell phones in the vicinity (Hosein and Palow 2013). Stingray devices are also able to intercept the contents of communications (Zetter 2015).

[36] Under federal law, both federal and state judges are required to report any law enforcement requests to intercept the contents of communications to the Administrative Office of the U.S. Courts, which then compiles them and publishes them on a yearly basis. These reports are often referred to as the *Wiretap Reports*, and contain detailed information in each request made by law enforcement.

cost of tracking the location of a suspect using a stingray and obtaining cell tower location data from cellular service providers. While it may cost over $70,500 to track a suspect for 28 days using a stringray device, the same surveillance using historical cell tower location data was estimated to cost between $30 and $2,800 depending on the cellular service provider (Bankston and Soltani 2014). As commercial entities continue to collect increasingly varied and detailed information about their users, law enforcement may be increasingly able to utilize low cost methods of electronic surveillance. Furthermore, the cost of this technology is likely to further decline in the future (Pell and Soghoian 2014).

2. Technical Capabilities and Capacities

In order to use a form of electronic surveillance, law enforcement must first know that this form of surveillance exists. While some forms of electronic surveillance are widely known, law enforcement officers may be unaware of newer surveillance options and therefore unable to employ them appropriately. Once the law enforcement officer knows a particular form of surveillance exists, they must also understand how to use it. For example, in order to use data gathered by smartphones in a criminal investigation, a law enforcement officer must know that the data is collected, who is collecting it, and how to contact this collector with a law enforcement request. However, this information may be hard to come by. While there are some resources that compile lists of appropriate law enforcement contacts at different communications companies (SEARCH.org 2016), this information is generally passed on from other law enforcement officers through email list-servs.

Law enforcement use of electronic surveillance is also limited by the scope of the available infrastructure devoted to electronic surveillance use. Many forms of electronic surveillance require access to specialized equipment. For example, use of a stingray requires access to the device, thus requiring law enforcement officers who want to use this form of surveillance to either purchase or borrow one. In some states this specialized equipment may only be operated by certain agencies at centralized locations, which creates bottlenecks in law enforcement surveillance processes. For example, all of the wiretaps for the entire state of Texas are conducted by the Texas Department of Safety in Austin. This facility has the capacity to monitor eight telephones simultaneously, which creates an upper limit on the number of wiretaps that can be operated simultaneously by state law enforcement (Strange 2015).

D. Literature Review

The interplay between technological innovations and Fourth Amendment legal protections more generally has been extensively studied. Many scholars have sought to explore how traditional legal protections for individuals targeted by law enforcement

searches may be (or many not be) affected by new technologies (Owsley 2013, Kerr 2004, Solove 2002), and suggest alterations to the current legal regimes to account for changes in technology (Henderson 2013). However, most of these analyses rely on legal and logical arguments rather than empirical data. To my knowledge, no research has yet been done on how law enforcement officers perceive laws as affecting their decisions to use electronic surveillance or request information from commercial entities.

There has been some scholarship exploring the role that resource constraints play on the decision to use electronic surveillance. For example, Minzner and Anderson (2013) used economic modeling "to test whether the warrant process actually limits investigations" in the context of wiretaps (pg. 171). They determined that it was the difficulty and expense of implementing a wiretap, rather than the requirement that law enforcement obtain a warrant before using a wiretap, that determined the intensity of wiretap use by law enforcement.

This research aims to contribute to the existing literature by empirically exploring how law enforcement officers decide to use electronic surveillance and commercial information requests through interviews with law enforcement officers that utilize these techniques. While the existing literature largely focuses on the role of legal and structural/practical restraints on law enforcement behavior, I seek to discover whether there are any other considerations that shape the decision to use electronic surveillance and commercial information requests. Understanding the considerations that shape the decision to use electronic surveillance and commercial information requests also sheds light on other critical policy questions, including the barriers faced by law enforcement officers who seek to use these techniques and the role that cost and other structural privacy protections continue to play in the this decision making process.

II. Data and Methods

A. Overview and Research Questions

In this paper, I explore how law enforcement officers make decisions regarding electronic surveillance. In particular, I seek to answer two related questions. First, how does law enforcement decide to use electronic surveillance and commercial information requests? Second, how is this decision making process different between electronic surveillance and commercial information requests?

To answer these questions, I conducted interviews of 23 law enforcement officers to determine how they use electronic surveillance and commercial information requests. In the remainder of this chapter, I describe how I developed my interview protocol, selected law enforcement officers to interview, conducted these interviews, and analyzed the results.

B. Sample

I sought to interview law enforcement officers who regularly engaged with electronic surveillance. Typically, these were mid-level or senior officers in an investigatory role. I focused particularly on officers who worked in divisions that were more likely to conduct surveillance, particularly those who investigated major crimes, narcotics, or cyber crimes. To recruit these officers, I obtained contact information for local police departments from cities across the United States. I started with police departments from large and mid-sized cities, and then continued to look at departments in smaller localities as I encountered difficulty locating willing interview subjects. If contact information for individual officers were not available, I contacted either the head of the agency or the public information contact person. All initial contacts were conducted via email. I contacted 349 departments, and yielded 23 interviews with law enforcement officers.

The officers interviewed were geographically diverse, hailing from 17 different states. 13% were from the Northeast census region; 26% were from the Midwest; 40% were from the South; 13% were from the West. Most of the officers interviewed were from local police departments; one was from a county agency and one was from a state agency. The local police departments mostly served small and medium sized communities; the average population size was 138,860; the standard deviation was 99,200. The officers interviewed were all highly experienced, and had generally been in law enforcement for years. Most were involved in investigatory roles in their departments; some were specifically tasked with implementing electronic surveillance but could speak to how the decision to use electronic surveillance was made. All but one of the officers interviewed were male.

C. Interview Protocol and Analysis

After informing interview subjects that they could refuse to be interviewed and obtaining consent, I conducted a semi-structured interview with each law enforcement officer to gather information about how they used electronic surveillance and commercial information requests. Semi-structured interviewing is used to elicit information when the researcher only has limited access to an interview subject, and facilitates the collection of information that can be compared across respondents (DiCicco, Bloom and Crabtree 2006). This technique is frequently used in criminal justice research (Copes, Brown et al. 2011). Given the geographic range of the interview subjects and the difficulty in scheduling interviews with law enforcement officers who are active investigators, all interviews were conducted by phone. Prior research has indicated that telephone interviewing does not result in the collection of substantially less rich data (Sturges and Hanrahan 2004). Wherever possible, interviews were recorded and transcribed.

However, some of the officers interviewed declined to be recorded. Careful notes were taken during all interviews, which allowed for analysis of the unrecorded interviews.

When developing the interview protocol, I consulted with several key informants – law enforcement officers or former law enforcement officers who were widely regarded to be experts in electronic surveillance. The use of key informant interviews to develop an interview protocol were conducted to help ensure that the questions made sense to the interview subjects, were likely to reveal relevant and interesting information, and to identify potentially sensitive areas. In this case, conversations with these key informants revealed that there were diverging opinions about what techniques should be considered to be electronic surveillance, and the differences between electronic surveillance conducted by law enforcement and law enforcement use of electronic surveillance conducted by commercial entities. Some informants were adamant that these techniques should be considered as separate categories, since they involved different types of law enforcement activities and were subject to different levels of legal regulation. Therefore, I crafted my interview protocol to tease apart these distinctions by asking about electronic surveillance and commercial information requests separately.

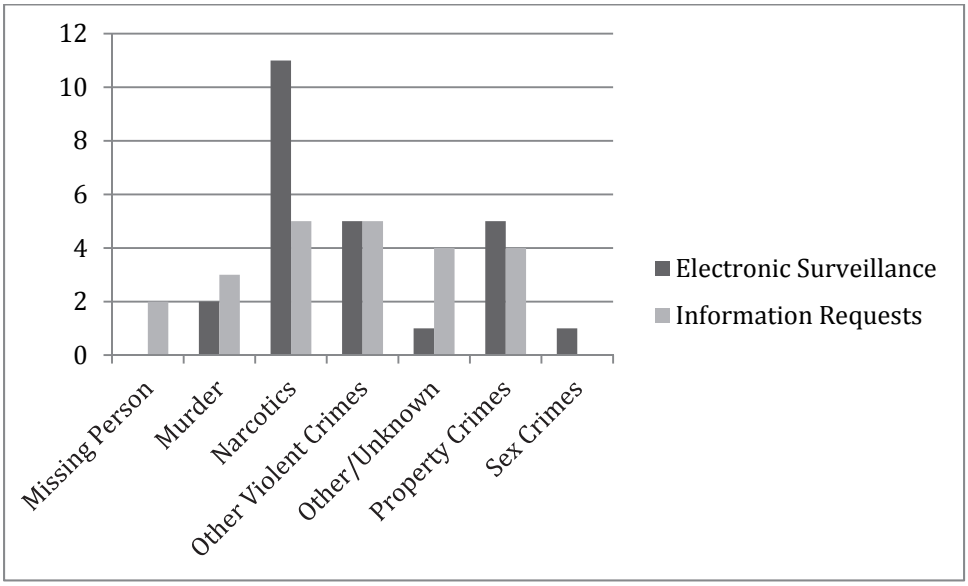
The final interview protocol consisted of three parts. In the first part, law enforcement officers were asked to explain how they would define electronic surveillance, and then provide a list of all forms of electronic surveillance that they could recall. In the second part, officers were asked to recall and describe the last investigation where they used electronic surveillance. Once they had provided an overview of this investigation, they were asked specific questions regarding the types of electronic surveillance used over the course of the investigation. For each type discussed, they were then asked to explain how it was used in the investigation and what they considered when making the decision to use it. In the third part, this process was repeated for the last investigation where the officer requested information from a commercial entity.

Figure 3.1 below describes the types of crimes under investigation in both the law enforcement narratives of electronic surveillance use and commercial information requests.[37] Most of the crimes discussed in these narratives were serious: almost half (11 out of 23) of the electronic surveillance narratives described investigating a narcotics crime, while almost a quarter (5 out of 23) were concerned with other types of violent crimes. Almost a quarter (5 out of 22) of commercial information request narratives were concerned with narcotics crimes, and almost a quarter (5 out of 22) dealt with other violent crimes. All-in-all, narcotics and violent crimes investigations accounted for more than half of electronic surveillance narratives, while murder, narcotics, and violent crime investigations accounted for more than half of the commercial information requests

[37] Because law enforcement may be investigating more than one type of crime simultaneously, these numbers do not sum to the total number of narrative elicited.

narratives. This comports with the general expectation from both policymakers and academics that electronic surveillance is primarily used to investigate serious criminal activity.

Figure 3.1. Types of Crimes Investigated[38]



Because the officers could use more than one search method over the course of an investigation, each interview could yield more than one description. The interview process yielded descriptions of 32 instances of electronic surveillance use and 22 instances of commercial information requests. Figure 3.2 below describes the types of electronic surveillance discussed during these interviews; figure 3.3 below describes the commercial information requests discussed. As can be seen, video surveillance was the most frequently used form of electronic surveillance, followed by the use of a GPS device to track a suspect's location. Phone records accounted for 40% of the commercial information request narratives.

[38] In comparison, of the 4,148 wiretap requests reported in 2015, narcotics crimes were the most serious crime under investigation in 79% of requests, homicide and assault in 5% of requests, and racketeering in 3% of requests. No other named category of crimes amounted to more than 1% of requests. Administrative Office of the U.S. Courts, *Wiretap Reports 2015,* Table 3, *available at* http://www.uscourts.gov/statistics/table/wire-3/wiretap/2015/12/31. The fact that the crimes reported in the *Wiretap Reports* are different from the crimes investigated in these narratives is unsurprising, as wiretaps have historically been used in particular types of investigations – especially narcotics investigations.

Figure 3.2. Types of Electronic Surveillance Discussed

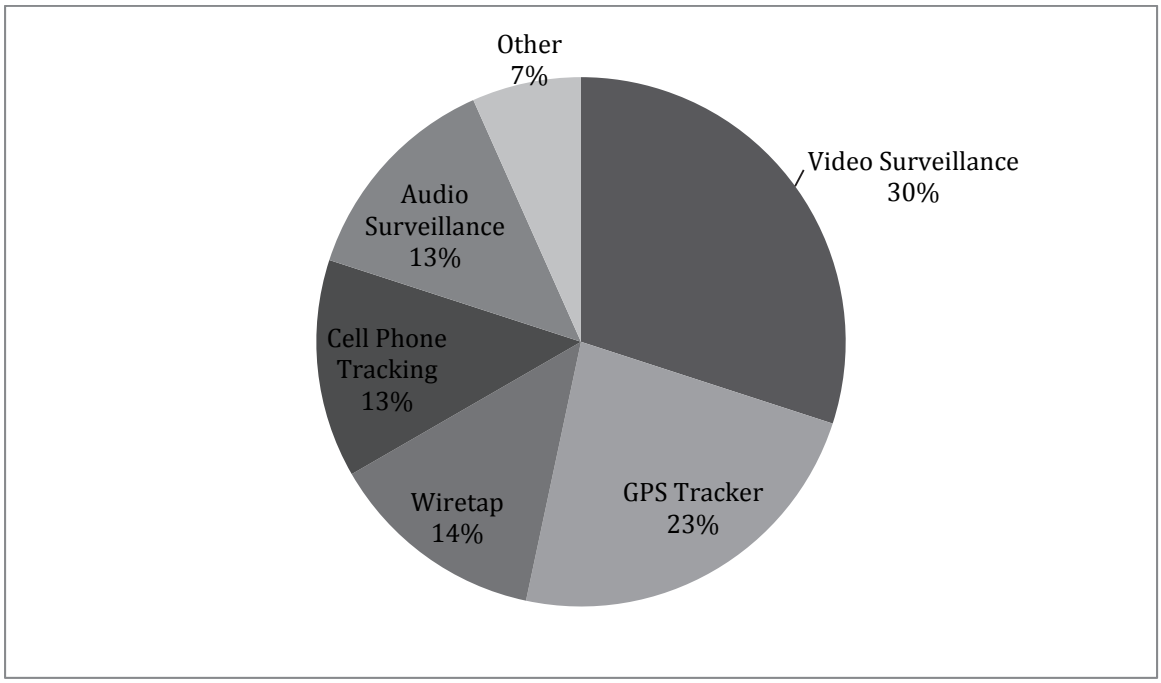
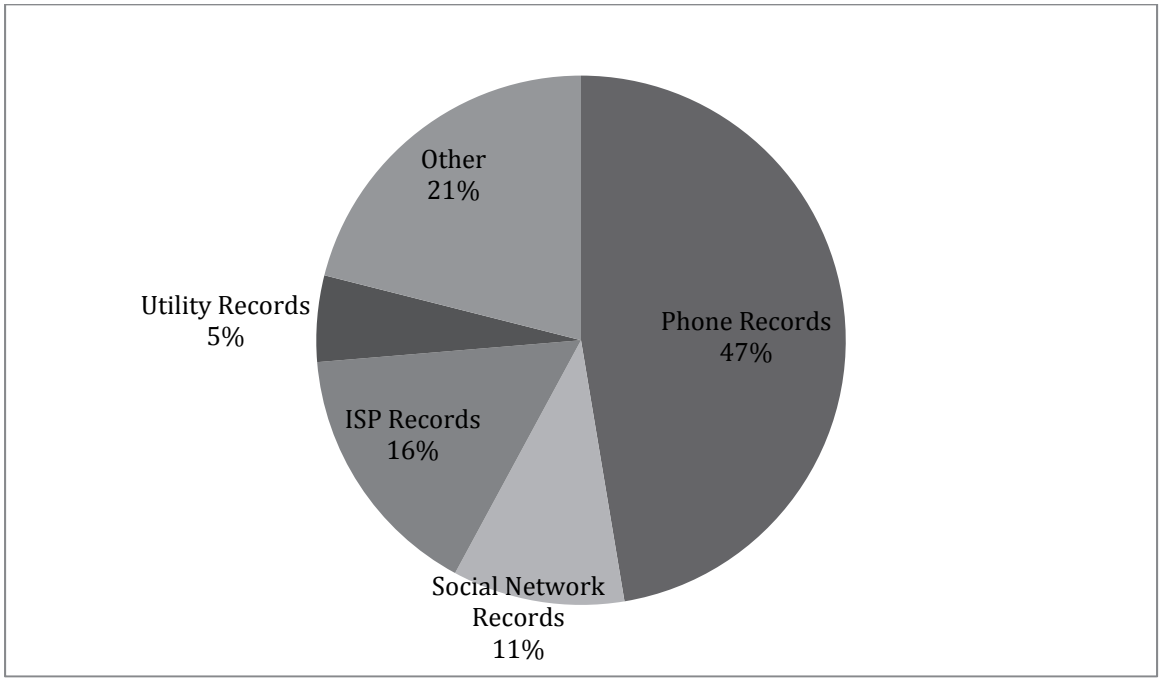


Figure 3.3. Types of Commercial Information Requests Discussed



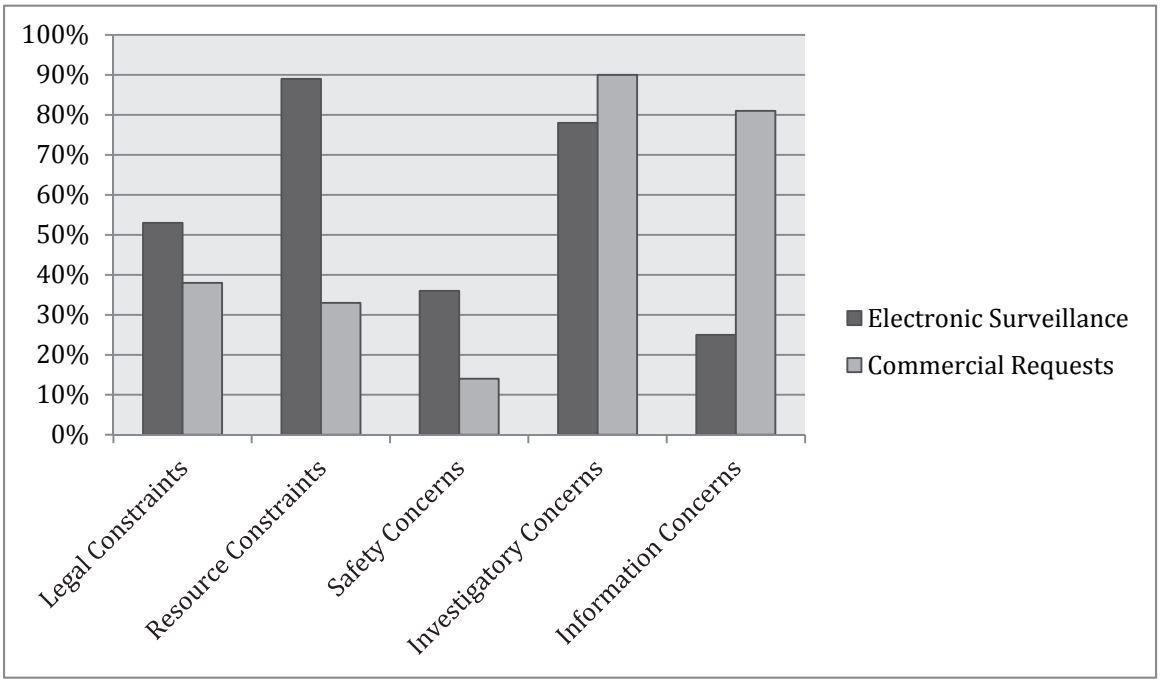
The transcripts and notes pertaining to each description of electronic surveillance use or commercial information request were read carefully and then coded for themes. Coding was conducted in two phases. First, I coded the interviews for themes that were

relevant to the policy problem and appeared across multiple interviews; this process was repeated by another coder to check reliability and validity. The observed rate of agreement between the two coders was 82%, well within the acceptable range (Campbell et al. 2013). This procedure yielded over twenty separate themes. Second, I sorted these themes into categories based on the underlying concerns they represented. This process yielded five separate categories, each pertaining to a different factor that the law enforcement officers interviewed considered when deciding to use electronic surveillance.

III. Results

Respondents provided an in-depth description of the factors they considered when deciding to use electronic surveillance. These factors were coded, and then grouped into themes based on the underlying concern they represent. Figure 3.4 below describes the types of factors that the law enforcement officers interviewed considered when deciding to use electronic surveillance or commercial information requests. In the remainder of this section, each category is described and discussed in depth.

Figure 3.4. Factors Considered When Deciding to Use Electronic Surveillance and Commercial Information Requests



A. Legal Concerns

When describing how they decided to use electronic surveillance or commercial information requests, some law enforcement officers considered the legal processes that must be followed in order to use electronic surveillance, such as a requirement to obtain a warrant or court order. I have describes these considerations as "legal concerns." This category encompasses both consideration of the relevant legal standard for using particular form of electronic surveillance or commercial information request, as well as contemplation of the legal uncertainties that might exist in a particular area. This theme is particularly salient because some scholars (and Supreme Court justices) have argued that legal concerns do not play as great a role in limiting law enforcement use of technological searches as resource constraints. Indeed, legal constraints were not a factor in almost half of the electronic surveillance narratives, and a majority of the commercial information request narratives.

1. Electronic Surveillance

About half of respondents considered the legal requirements (such as obtaining a warrant or subpoena) that must be met in order to use electronic surveillance. Legal restraints were discussed as a consideration in 53% (N=19) of the instances of electronic surveillance use discussed. Even though legal requirements were something that law enforcement officers considered when deciding to use electronic surveillance, it did not

always appear that law enforcement always viewed these requirements as a barrier to using electronic surveillance. Rather, compliance with the law is seen as part of how law enforcement officers structure their investigations. As one officer described, "that's just the way we conduct out investigations from beginning to end…we tick off all these steps that we know we'll have to have when it comes time to do our application." Some officers even discussed legal requirements as improving the quality of investigations, rather than as an impediment to effective police work. One officer explained that "having to get a warrant forces you to do a lot more legwork in the beginning and build a stronger case because you are going to have that judicial oversight. It makes you…a better cop."

Law enforcement officers may be concerned with legal restraints on electronic surveillance use because the law in this area is constantly evolving. In the face of legal uncertainty, some law enforcement officers may decide to seek to obtain legal permission to use electronic surveillance, even if they are unsure that this permission is required. For example, when discussing why he considered legal requirements when deciding to use a GPS tracker, one respondent explained:

> "I think at first, it was just the wild west, because the law hadn't caught up to the technology. But over time, there have been some regulations and some court rulings, that have restricted law enforcement…No matter what we do, if you've got probable cause, it doesn't matter, you can get a warrant and move forward that way, and err on the side of caution. My thought process is always, even if it's slightly controversial, I'll get a search warrant, or some other legal exception to search."

While there is no evidence on the extent to which law enforcement officers seek legal permission to use electronic surveillance when they are uncertain that such permission is required, this practice suggests that law enforcement may behave more conservatively when faced with legal ambiguity.

2. Commercial Information Requests

The law enforcement officers interviewed considered the applicable legal constraints in 27.27% (N=6) of the narratives describing commercial information requests. In general, law enforcement officers described legal protection for information as a factor in their decision, but not as a reason to forgo requesting information from commercial entities. As one officer interviewed noted, "the last thing we want to do is lose a case, or have evidence thrown out, because we cut a corner or something like that. It's not really that hard to write a search warrant, to subpoena records, and things of that nature." Additionally, one law enforcement officer explained that complying with stricter legal standards may simplify some aspects of requesting commercial information, because it can prevent objections from the commercial entities. The officer explained that requiring

a court to review requests to use commercial information "it's just one more step for us but, in my opinion, it helps us to show that we're not just doing fishing expeditions."

B. Resource Concerns

The law enforcement officers interviewed also discussed both the costs of using electronic surveillance and the resources available to pay those costs. Potential costs include both the financial cost of undertaking the surveillance, the manpower required to implement the surveillance technique, and the probability of losing or destroying the surveillance equipment. Potential resources include the surveillance equipment already owned by the department and the possibility of external funding. Resource concerns were discussed in a majority of the descriptions of electronic surveillance use, but not in a majority of descriptions of commercial information requests.

1. Electronic Surveillance

In 89% of instances (N=32), resource availability was discussed as a factor in the decision to use electronic surveillance. According to some officers, cost is an inevitable concern, because "we don't have unlimited funds to do things." Respondents identified several sources of electronic surveillance costs. Electronic surveillance generally requires specialized equipment, which can be quite expensive. According to another officer interviewed, "the infrastructure behind a lot of the surveillance is costly, which can deter smaller agencies from utilizing it." Additionally, some types of electronic surveillance can generate enormous amounts of information and, in some situations, law enforcement may be required by law to maintain evidence for a long period of time. One officer described data storage as "the biggest issue we've found", especially because of the associated cost.

Manpower requirements are related to the cost of using surveillance. For example, one officer explained that electronic surveillance could help reduce the costs of conducting an investigation, because "if [he] had to put four, five, six guys on somebody and follow them around 24/7, that could get very expensive very quickly, as opposed to putting on a GPS tracker and then going back afterwards and seeing what happened." Electronic surveillance also helps law enforcement avoid the opportunity cost of conducting surveillance. As one officer described, using electronic surveillance helps law enforcement "keep[] guys fresh and still able to do our other investigations at the same time." However, certain types of electronic surveillance may require a non-trivial amount of manpower, as they involve equipment that must be maintained in the field.

Law enforcement officers also considered both the internal and external resources available to them when deciding to conduct electronic surveillance. For example, some officers considered what electronic surveillance equipment that had already been purchased by their department. As one officer interviewed explained, "if you buy a

bicycle and you ride it around the block one time or you ride it around the block ten times, you still have the bicycle. So the equipment we have is good to make 100 cases or to make 1,000 cases." Additionally, some officers considered whether they could obtain assistance from federal or state agencies. One officer explained that his department had "very good relationships with some federal agencies, and if I need something that we don't have, I can obtain it from them – they will lend it to us."

2. Commercial Information Requests

Some law enforcement officers interviewed discussed resource constraints as playing a role in their decision to use commercial information requests. 33% (N=7) of law enforcement officers interviewed described cost as a consideration in their decision to request information from commercial entities. One officer explained that he considered the cost of requesting information relative to the probability that this investigation will result in a prosecution. According to this officer, "if at the end of the day I spend ten hours on an investigation, and I know that even if I get the person, that it's not going to be prosecuted, that's not a going to be a wise use of time or resources." Law enforcement officers were particularly concerned about the cost of analyzing information. While "you could go crazy and send subpoenas and search warrants out all day long, but in the end, someone needs to go through these records and make sense of them – analyze them and be able to put that information to good use." When costs were not a factor, this was often because the officers saw other priorities as more pressing. "When it has to do with someone's health and well-being, then there is no consideration."

C. Investigatory Concerns

Electronic surveillance and commercial information requests are not made in isolation; they are intended to further a particular criminal investigation. Unsurprisingly, the law enforcement officers interviewed frequently considered the broader investigation when deciding to use electronic surveillance or commercial information requests. I therefore use the term "investigatory concerns" to describe discussion of the context of the investigation and the role of the technique in it. These investigatory concerns included whether the technique could produce evidence that would be particularly convincing at trial, and whether electronic surveillance or commercial information requests could help law enforcement achieve the goals of the investigation.

1. Electronic Surveillance

The officers interviewed often discussed how the particular investigation before them affected their decision to use electronic surveillance. Concerns about the investigation were a factor in the decision to use electronic surveillance in 78% (N=28) of the instances of electronic surveillance use discussed. In addition to considering the facts of the case,

law enforcement officers interviewed articulated a variety of other specific investigatory concerns that affected their decision to use electronic surveillance. For example, some officers appeared to conduct a cost-benefit analysis to determine whether utilizing electronic surveillance was justified by the severity of the crime committed. One officer interviewed discussed the difficulties associated with obtaining legal permission to use a form of surveillance, and then explained that he would not "do that for some misdemeanor crime that somebody is going to get a $100 fine on."

Some officers considered whether they could use the evidence obtained from electronic surveillance to further develop the investigation or prosecution. One officer explained that he decided to use a GPS tracker, because he thought that the information he could obtain was "important for the development of possible future search warrants, so we could develop the probable cause" necessary to conduct a search. Another described seeking video recordings of criminal activity because they were particularly convincing at trial, since "if [the jury] actually see people diving for the floor, jumping on or holding their kids, then that helps show them the severity of the crime we're dealing with."

Some law enforcement officers interviewed also considered whether could obtain information about a case without using a particular form of electronic surveillance. For example, one officer explained that he had decided to use a pole camera to monitor a location where criminal activity was occurring because "it got into an area where we could not physically get in the area and watch without it being obvious."

2. Commercial Information Requests

90% (N=19) of law enforcement officers interviewed discussed how characteristics of the investigation affected their decision to request commercial information. For example, one officer explained that his "biggest consideration…is what is the criminal act that we're investigating." He went on to explain that he viewed this as a concern because determining that a crime had been committed was a necessary prerequisite to obtaining a subpoena for commercial information. Other law enforcement officers interviewed explained that they considered how the information obtained through a commercial information request would fit in with their subsequent investigation, particularly whether the commercial information sought could be used to further an investigation by allowing law enforcement to obtain a warrant to conduct further searches.

D. Safety Concerns

Law enforcement officers are frequently concerned with the safety of both law enforcement officers and the general public. The officers interviewed discussed how concerns about safety affected their decision to use electronic surveillance or commercial information requests. For example, law enforcement may decide to use a GPS location tracker on a car because following in a chase car is risky for both the officers driving the

car and other motorists. Although it appeared in a minority of either type of narrative, safety concerns were mentioned more frequently in the context of electronic surveillance than commercial information requests.

1. Electronic Surveillance

In 36% (N=13) of the instances of electronic surveillance use discussed, safety was a consideration in the decision to use electronic surveillance. The law enforcement officers interviewed discussed how both officer safety and public safety drove their decision to use electronic surveillance. As one officer described, "in our business, we always say safety of the public, safety of ourselves that's the primary concern." Electronic surveillance was seen as a mechanism for investigating crimes with lower risk to law enforcement officers. For example, one officer explained that using GPS technology to help track a suspect's vehicle "allows [them] to back off further if we're doing physical surveillance, and minimize the chances of them noticing the physical surveillance…[which] can be dangerous." However, electronic surveillance use does not eliminate all risk to law enforcement. In particular, several law enforcement officers interviewed talked about the risks associated with planting a tracking device on a car, which one described as "a dicey situation at times." However, law enforcement may be able to minimize these risks. For example, one officer explained that they often try to find cars similar to the suspect's car, so that they can practice placing the tracker quickly and surreptitiously.

2. Commercial Information Request

Safety considerations generally did not play role in the decision to use commercial information. Only three (14%) officers interviewed discussed safety concerns as a factor in their decision to request information from a commercial entity; in all three cases, the officers discussed the need to protect public safety rather than the safety of law enforcement officers. Safety tended to be a factor in the decision to use commercial information when the subject of the information was thought to be dangerously violent. For example, one officer said that, given the suspect was thought to be violent, they "wanted to know as much as possible about what this person has done and had been involved in."

E. Information Concerns

The goal of both electronic surveillance and commercial requests is to obtain information that may help law enforcement conduct a criminal investigation. However, not all information is equally helpful to an investigation. Some law enforcement officers interviewed considered the type and quality of the information they would obtain through using electronic surveillance or a commercial information request. For example,

discussion of the resolution and retention of the information yielded by a particular technique were included in this category, since these are characteristics of the information obtained from electronic surveillance or the commercial information request. Information concerns were mentioned much more often in the context of commercial information requests than electronic surveillance.

1. Electronic Surveillance

Concerns about the information that could be obtained through the use of electronic surveillance were discussed in 25% (N=9) of the narratives. These information concerns included the type and quality of the information that could be obtained by using electronic surveillance. One officer interviewed also discussed considering the speed with which information could be obtained. In that particular instance, the officer described using electronic surveillance to locate a suspect they believed was an on-going threat. They decided to use electronic surveillance because it "was the quickest way to locate him and to neutralize whatever potential threat he could be."

2. Commercial Information Requests

The law enforcement officers interviewed frequently described concerns about the information they could obtain using commercial information requests. In 90% (N=19) of the commercial information request narratives, the law enforcement officer discussed the role that the type, quality, and availability of information played in their decision to use commercial information requests. In particular, the accuracy, reliability, and freshness of the information were all concerns. For example, one officer interviewed mentioned that he often tried to verify information he got from commercial sources through other means, and described this practice as "just Investigations 101": "you never trust any one source, you always corroborate your information."

A necessary step in obtaining commercial information is identifying a commercial entity who may have information relevant to a case. According to some officers interviewed, certain commercial entities are generally known to be antagonistic to law enforcement requests for information, while others are cooperative. For example, one law enforcement officer described a company who could potentially have information relevant to a case as "time consuming and difficult to follow up", while another explained that he knew the company he sought information from was "really good…they're 24/7 on their law enforcement line." However, even if the commercial entity is known to be challenging to obtain information from, law enforcement officers do not necessarily see this as an insurmountable barrier. As one officer described, "they can try to be difficult, but it's still our job to do whatever we can to get that information if that's what's going to be able to solve a case."

IV. Discussion

A. Description of Law Enforcement Decision Making

As expected from the literature, the law enforcement officers I interviewed identified legal requirements and resource constraints as factors in their decision to use electronic surveillance and commercial information requests. However, while legal requirements were discussed as a factor in the decision to use electronic surveillance and commercial information requests about as frequently, resource constraints were mentioned much more frequently in descriptions of electronic surveillance then descriptions of commercial information requests. This apparent difference may be explained by the fact that it is generally more expensive to conduct electronic surveillance than request information from commercial entities.

My research also revealed three new factors that law enforcement considers when deciding to use electronic surveillance that are not commonly discussed in the literature. First, concern for the safety of both law enforcement and the general public was identified as a concern both in the context of electronic surveillance and commercial information requests. Electronic surveillance was described as a way for law enforcement to obtain information about a case with lower risk to human safety. This concern suggests that there may be previously unrecognized benefits to electronic surveillance. Not only can law enforcement use this technique to obtain information cost effectively, but they can also reduce the risk involved with any criminal investigation. In future analyses of the costs and benefits of using electronic surveillance, it may be advisable to account for the safety improvements that can be gained by using electronic surveillance rather than physical surveillance.

Second, the law enforcement officers interviewed frequently described considering the context of the investigation when deciding to use electronic surveillance and commercial information requests. On one hand, this is unsurprising: it is to be expected that law enforcement would consider the background and goals of the investigation when deciding to use electronic surveillance and commercial information requests. On the other hand, some of the specific considerations mentioned by law enforcement suggest that the context of a particular investigation may have a more nuanced impact on the decision to use electronic surveillance than one might expect. Some law enforcement officers interviewed discussed considering subsequent types of surveillance that might be available to them when they were deciding to use electronic surveillance; for example, whether requesting phone records might make it possible for them to request a wiretap further along in the investigation.

This suggests that the types of electronic surveillance used during an investigation may be path dependent. Path dependence is a concept that is used broadly, in everything from physics (Gosche and Steiner 1994) to political science (Pierson 2000), to refer to

situations where the impact of moving into a particular state depends on how the state was reached. In other words "path dependence refers to the causal relevance of preceding stages in a temporal sequence" (Pierson 2000, pg. 252). In the context of electronic surveillance, this suggests that the electronic surveillance options available to law enforcement may depend on the previous types of electronic surveillance used or (more subtly and perhaps more significantly) the benefits of using a particular type of electronic surveillance will depend on the previous types of electronic surveillance used. The previous choices made by law enforcement determine the choices that are available to them now, and potentially the probable outcomes of those choices.

For example, law enforcement officers may be more likely to intercept a suspect's communications if they have previously obtained metadata about the communications that demonstrate that communications may be incriminating. Additionally, law enforcement may be able better able to obtain incriminating information from intercepting a communication after obtaining metadata about the communication, since they already have knowledge about the communications they are trying to intercept. While path dependence in electronic surveillance has a great amount of intuitive appeal, it has not been thoroughly explored[39] in the literature or carefully considered in policymaking.

Finally, law enforcement officers described considering the type and quality of information they would obtain by using electronic surveillance and commercial information requests; however, this factor was mentioned much more often for commercial information requests than electronic surveillance. When law enforcement obtains information from a commercial entity, they may have little control over the type and quality of the information they receive, the difficulty of working with the commercial entity that has the information, and the speed with which they receive the information.

---

[39] There are some references to the need to maintain "building blocks" of electronic surveillance: intermediary forms of surveillance that do not require a warrant, but can yield information that will support a warrant for more invasive surveillance. However, these references generally do not provide evidence or analysis to support the theory that these building blocks are needed. For example, Dempsey (2012) argues that "ECPA reform must preserve the building blocks of the investigative process: the subpoena for subscriber identifying information and other basic information, the court order issued under §2703(d) on less than probable cause for Internet transactional information, and the warrant for communications content and other highly sensitive information. It is important that investigators have the ability to work their way up that ladder of authority, gaining access to more sensitive data as the standard increases." This discussion is proscriptive rather than descriptive. Further research is needed to understand how (and under what circumstances) interactions between different types of surveillance may occur.

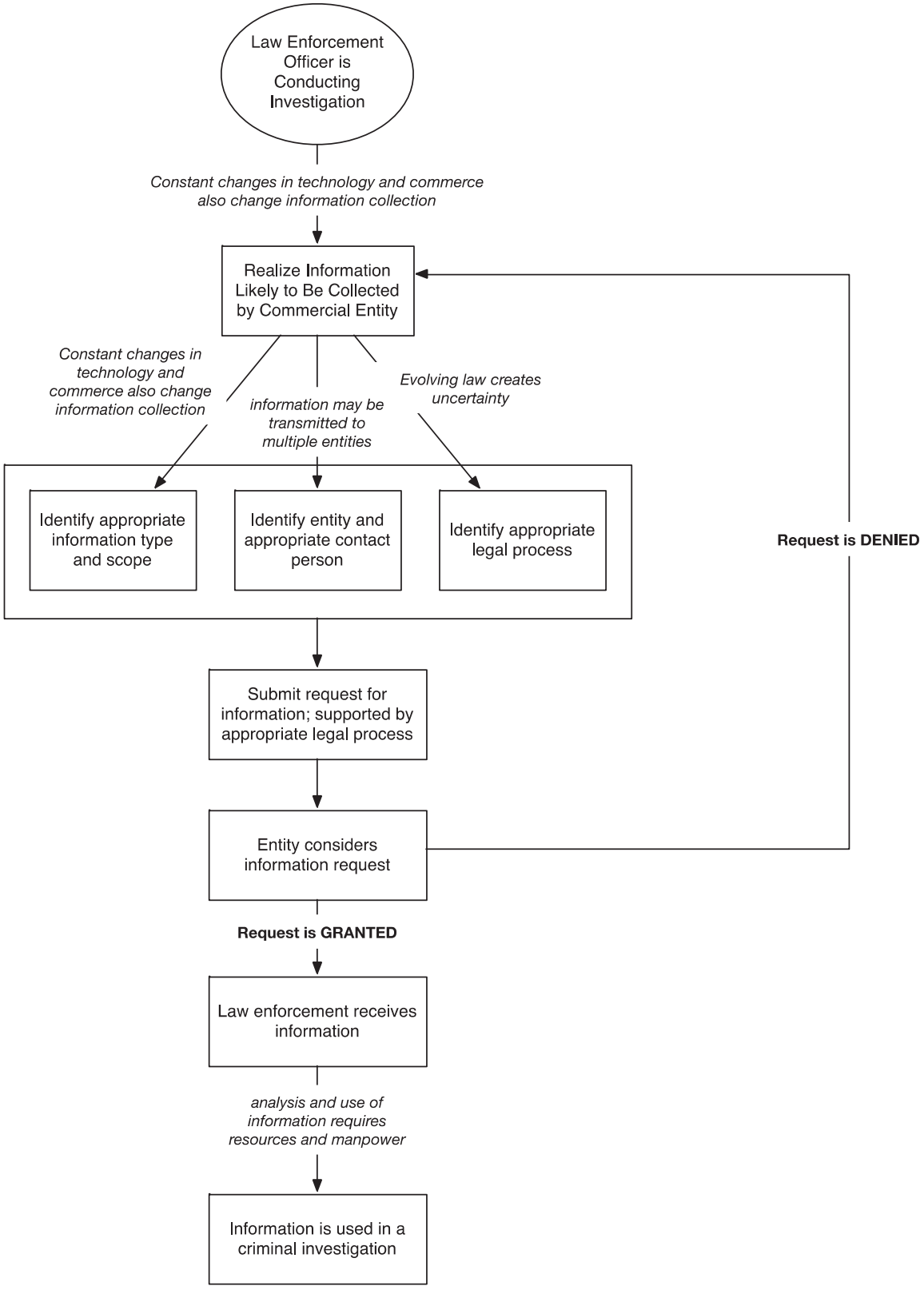
Consequently, these concerns are much more salient in the context of commercial information requests than electronic surveillance.

B. Technological Search Methods are Not Self-Executing

Electronic surveillance and commercial information requests are often thought of as tools that allow law enforcement to conduct criminal investigations more effectively. In particular, electronic surveillance has been described as a force multiplier: "a factor that dramatically increases the effectiveness of an item or group" (Patton 2011). However, analyses of the impact of electronic surveillance and commercial information requests may underestimate the amount of active law enforcement participation required to use electronic surveillance or commercial information requests. Even though electronic surveillance may require less in-person activity than traditional forms of surveillance, one respondent noted that law enforcement "can't use any electronic surveillance without putting boots on the ground." Indeed, significant resources may be required to implement electronic surveillance, particularly to ensure that it is implemented safely and in accordance with legal protections for individual rights.

For example, it may appear that by requesting information from commercial entities, rather than collecting it themselves, law enforcement can avoid many of the difficulties described above. However, commercial information requests implicate a new set of barriers for law enforcement. Figure 3.5 below describes a logical model of the steps law enforcement will generally follow in requesting information from law enforcement; the italicized text represents the barriers that they must overcome before they can use the information in a criminal investigation.

Figure 3.5. Logical Model of Commercial Information Request



Before law enforcement can request information from commercial entities, they must first realize that information pertinent to their case has been collected by commercial entities. While law enforcement familiar with sources of commercial information that have been around for many years, they may not realize the full potential of newer sources of information. For example, while many officers will realize that they can request information from the phone company, they may not be aware of the breadth and depth of information they can request from mobile application developers (Balkovich et al. 2015).[40] While newer sources of commercial information may provide richer data than traditional sources, law enforcement officers may not be well-positioned to take advantage of these developments.

After determining that information relevant to their case may have been collected by a commercial entity, the officer must then determine which commercial entity is likely to have the information, and identify the appropriate contact person at that agency. According to one officer interviewed, this process can be "an adventure in and of itself." A single consumer device can share information with multiple commercial entities. For example, if law enforcement is interested in using information collected by a smartphone to determine whether the suspect had contact with the victim, he could seek information from the phone company that provides service to the phone, the manufacturer that produced the phone, or the developers who created communication apps found on the phone. One officer interviewed described the confusion that this plurality of data sources may cause: "Who do I even have to start the paperwork trail with? So if somebody has a service provider and their service provider is AT&T… [does that mean that] it's AT&T you're serving records to…or if they're using Facebook, do I have to subpoena AT&T and Facebook?"

Additionally, law enforcement must determine what type of information they will request from the commercial entity. This is not always as simple as it seems. Some entities may require specific technical information in order to locate the proper record, or may only comply with legal documents that correctly specify the formal name of the information requested. Law enforcement may need to repeat their request several times before the commercial entity will comply. According to one officer interviewed, the commercial entity "might call back and say, 'Oh, you didn't ask for the right thing. You're getting nothing. Resubmit a new warrant or a new thing, a new request.'" This process can be particularly arduous for smaller law enforcement agencies, which may

[40] This barrier is likely to be lowered over time, as law enforcement departments become more aware of their options for obtaining information from commercial entities. However, as the amount, type, and breadth of information collected by commercial entities is increasing rapidly, the lowering of this barrier may not occur as quickly as one might expect.

request commercial information less often and may therefore be less familiar with the procedures.

After the appropriate commercial entity has been identified, law enforcement must then submit a request for information, accompanied by the appropriate legal document. Under some circumstances, this can be a fairly straightforward process. One officer explained that this is "a relatively simple process now…we will prepare a court-ordered subpoena…[and] usually we're pretty successful in getting what we need." However, the law governing law enforcement access to commercial information is developing rapidly and may vary significantly from state-to-state. Law enforcement may therefore face difficulty in determining which law is applicable to a given situation.

After law enforcement has obtained the information from the commercial entity, they must then examine it and determine whether and how it applies to their investigation. Commercial entities can collect huge amounts of information about their customers, particularly when selling this information is an essential part of their business model. Law enforcement agencies have limited resources to analyze this information, and may not be familiar with the computational analytic techniques often used by commercial entities to create insights from data. As one officer interviewed explained

> We have a limited amount of manpower. And you could go crazy and send subpoenas and search warrants out all day long, but in the end, someone needs to go through these records and make sense of them – analyze them and be able to put that information to good use….it takes someone to sit down and go through all of this and try to make sense of it.

The manpower required to parse the results of commercial information requests may serve as a natural limitation on the scope and frequency of law enforcement requests for commercial information.

C. Cost remains a factor in the decision to use electronic surveillance

Improvements in technology have undoubtedly made electronic surveillance less expensive for law enforcement. As estimated by Bankston and Soltani (2014), covert car pursuit of a vehicle would cost approximately $184,800.00 over the course of 28 days, while use of a GPS tracker to obtain similar information would cost approximately $240.00 – approximately 0.1% of the cost of covert physical surveillance. Given the potential cost differential between physical and electronic surveillance, it seems reasonable to ask whether cost provides a meaningful limitation on modern electronic surveillance.

Many law enforcement officers interviewed described cost as a consideration when deciding to use electronic surveillance. In fact, several officers appeared to describe conducting something akin to a cost-benefit analysis before deciding to use surveillance,

particularly with regards to the manpower required. One officer explained that "there are many cases where we could use electronic surveillance and we don't, because it's the time and effort that you have to put in and it's kind of risk versus reward." Law enforcement seemed particularly unlikely to use electronic surveillance if they did not think that it would be prosecuted or could yield a conviction. According to one officer interviewed, "at the end of the day, [if] I spend ten hours on an investigation, and I know that even if I get the person, that it's not going to be prosecuted, that's not going to be a wise use of [my] time or resources."

There are several reasons why cost may remain a limitation on law enforcement use of electronic surveillance, even though the costs of conducting electronic surveillance are significantly lower than the costs of conducting physical surveillance. First, reducing the cost of electronic surveillance may not reduce structural protections if the cost of surveillance remains outside the budget of a many law enforcement agencies. This rationale implies that the extent to which cost remains a limitation on law enforcement use of electronic surveillance depends on the type of law enforcement agency conducting the investigation. Law enforcement agencies vary greatly in terms of size, budget, number and type of crimes to investigate, and population served. It may be that, even after technology has reduced the cost of using a certain form of electronic surveillance, it remains to expensive to use on a regular basis.

Second, it is necessary to consider the cost of electronic surveillance as it is actually used. As is shown in section (B) above, implementing electronic surveillance safely and covertly may require more manpower then would simply be needed to install the electronic surveillance device. While electronic surveillance may still be less expensive than physical surveillance, even after accounting for the cost of implementation, these additional costs may put it outside the reach of smaller agencies with fewer resources.

Third, different type of costs may affect law enforcement behavior differently. Some costs, called fixed costs, must be incurred once before any surveillance can be used, but do not increase as the amount of surveillance increases. Other costs, called variable costs, scale with the amount of surveillance used. A given type of surveillance may include both fixed and variable costs: law enforcement may need to first procure a device (fixed cost) and then pay for every hour it is operated (variable cost). Many analyses of the effect of cost on law enforcement decision making explicitly exclude fixed costs (Bankston et al. 2014). However, fixed costs also play a role in regulating law enforcement use of surveillance. Fixed costs could be expected to have a binary effect on law enforcement electronic surveillance decision-making: law enforcement must either opt in or opt out of using the technique. The effect of fixed costs on electronic surveillance use is particularly interesting because it may place limitations on smaller agencies that cannot afford to pay the fixed cost while allowing unlimited surveillance use by larger agencies. For example, a Stingray II cost over $130,000 in

2013 (Gallagher 2013). While this cost could be borne by larger agencies, it may be outside the resources of smaller and mid-sized agencies. Consequently, resource constraints would place few if any limitations on use of Stingrays by larger agencies, but would prevent smaller agencies from using Stingrays at all.

Fourth, even if a law enforcement agency can afford to use electronic surveillance, they may determine that the value provided by the use of electronic surveillance is not worth the cost in a particular case. For example, law enforcement officers may be reluctant to invest the resources necessary to conduct electronic surveillance when investigating a minor crime. One officer noted that "[i]f I'm looking at a couple of guys that are smoking weed on the porch, I'm obviously not going to want to expend the resources for a pole camera or something like that." Even though this officer had the resources available to obtain a pole camera and knew the pole camera would provide him with information on a criminal act, he determined that the value of obtaining this information was less than the cost of using electronic surveillance.

D. New Structural Protections for Privacy

While technological innovation may reduce existing structural protections for privacy, it may also introduce new sources of structural protections. In addition to the role of cost (as discussed above), the law enforcement officers interviewed discussed several structural limitations on their abilities to use electronic surveillance and commercial information requests that have been made possible by new technologies. In this section, I identify and discuss these potential new structural protections for privacy.

1. New Limitations on Electronic Surveillance

The same technological trends that make it easier for law enforcement to conduct electronic surveillance may also make it easier for criminals to evade that electronic surveillance. Several law enforcement officers interviewed discussed countermeasures that criminal suspects took to avoid electronic surveillance. For example, one officer explained that narcotics sellers "would change their telephone number about every two weeks…because they became savvy to law enforcement practices." This method of evading law enforcement surveillance is only practical because cellular technology has developed to the point that cell phones can be purchased cheaply, easily, and anonymously. Because criminals have as much incentive to take advantage of improvements in technology as law enforcement officers, the limitations created by counter-surveillance may keep pace with innovations in electronic surveillance, while law may be slower to recognize and respond to this counter surveillance.[41]

[41] For example, some lawmakers have proposed legislation to prevent anonymous purchasing of pre-paid cell phones (H.R. 4886 (2016))

2. New Limitations on Commercial Information Requests

As the number of commercial entities routinely collecting data about their customers has grown, so has the information potentially available to law enforcement. However, accessing these new sources of information may require technical knowledge that many law enforcement officers currently do not possess. As one officer interviewed noted

> I don't think we can expect your average police officer to understand the difference between an IMEI and an IMSI. You know, you can't ask them what the IP for your computer is, or your internet provider…. Most of us don't know those things. Most of us aren't going to know exactly what to ask for in a Facebook warrant.

If law enforcement cannot correctly and narrowly specify the technical parameters of their search, then they may either be denied judicial permission to collect information or experience resistance from the commercial entity. The technical complexity of obtaining data may be a new source of structural privacy protections for commercial information.[42]

To an extent, this structural barrier can be minimized by additional training and support of law enforcement officers. Some officers interviewed discussed resources they used to improve their ability to obtain commercial information requests; in particular, one respondent cited the resources available through the National White Collar Crime Center. Officers may also share information among themselves, both formally and informally. However, the need for additional training and resources increases the cost of using commercial information requests, and therefore increases the structural protections for this information. Additionally, technical training may not be sufficient to allow law enforcement officers to readily request information from commercial entities. According to one law enforcement officer interviewed "I think that we have very educated cops…But even then, unless they do this all the time, they're not going to know exactly what to ask for." This problem is compounded by the rapid technical development of commercial information collection. Training in locating and requesting commercial information may go stale quickly, and it may therefore be expensive to maintain law enforcement expertise in this area.

V. Limitations

This study has several limitations. First, this research differentiates between two types of surveillance mechanisms – electronic surveillance and commercial information

[42] This barrier is likely to be lowered, as law enforcement officers become more accustomed to requesting information and become more aware of what types of information to request. However, at the same time, new sources of information will continue to be developed, thus bringing new forms of technological complexity. Whether or not these barriers fall may depend on which increases more quickly: law enforcement knowledge or technological complexity.

requests – based on how the law enforcement officers I interviewed understand those terms. In a sense, this distinction is both too much and not enough. As the line between the type and quality of information that law enforcement can obtain through electronic surveillance as compared with commercial information requests has become increasingly fine, differentiating between these two techniques may obfuscate how similar they are in practice. Through this lens, the distinction between electronic surveillance and commercial information requests may seem like a false dichotomy. On the other hand, electronic surveillance and commercial information requests are sharply different if viewed through historical or legal lenses. It may seem that this paper should be limited to either electronic surveillance or commercial information requests, and discussing them both together simply invites confusion.

While the definitions of electronic surveillance and commercial information requests used in this work are imperfect, they are necessary. A member of the general public would probably define electronic surveillance much more expansively than a law enforcement officer – and, indeed, a generalized law enforcement officer might define electronic surveillance much more expansively than an officer well versed in the use of electronic surveillance. However, for purposes of this work it was necessary to craft an explicit definitional framework for the sake of clarity; adopting the internal perspective of law enforcement officers helps my analysis describe their decision making process. The shortcomings of my definitions of electronic surveillance and commercial information are a characteristic of the inherent disagreement in what should be considered electronic surveillance, not an artifact of my definitional scheme.

The second limitation is that this study relies on information collected from interviews with law enforcement officers, rather than observation of their behavior. Consequently, it will only reveal drivers of law enforcement behavior of which law enforcement officers are consciously aware. For example, if law enforcement officers subconsciously consider the age of the suspect when deciding to seek information from commercial entities, because they assume that younger persons are more likely to use devices that collect customer information, this consideration will not be reflected in the interviews because it is not an explicit part of their thought process.

Additionally, this research is based on a small, non-random sample of law enforcement officers, primarily from small and medium sized agencies. Therefore, it should not be viewed as representative of either law enforcement agencies generally, or law enforcement agencies that regularly use electronic surveillance specifically. In particular, it should not be viewed as representative of very large agencies that regularly and extensively engage in electronic surveillance, such as the New York Police Department.

However, neither of these limitations detracts from the significance of this research. Additionally, the primary goal of this research was to identify a range of considerations

that appear to affect electronic surveillance decision making, not to determine the prevalence of these considerations across electronic surveillance use in general. The law enforcement officers interviewed were selected to maximize the likelihood that they could provide insights into electronic surveillance decision making, rather than as representatives of law enforcement agencies in general. This yielded a richer list of the considerations that may drive use of electronic surveillance and communications intercepts. Furthermore, the fact that officers were chosen from smaller agencies also increases number of potential electronic surveillance considerations identified by this research. Smaller agencies often have smaller budgets and less experience dealing with electronic surveillance, and therefore officers from these agencies may need to be more deliberative in their decision to use electronic surveillance.

VI. Conclusion and Policy Implications

While law enforcement use of electronic surveillance and commercial information requests is a source of much policy concern, little is currently known about how law enforcement officers make decisions regarding these investigative techniques. This research aims to address that gap, by describing how law enforcement officers decide to use electronic surveillance and commercial information requests. Based on interviews with 23 law enforcement officers who engage with electronic surveillance regularly, I discovered and described five factors that law enforcement took into considerations: legal concerns, resource concerns, safety concerns, investigatory concerns, and information concerns. While the first two are discussed in the literature, the last three are previously unknown. I also use the results of my interviews to address several issues underlying the policy debate in this domain. I argue that technological search methods are not self-executing, and that both electronic surveillance and commercial information requests may require significant involvement from law enforcement officers. I also discuss the ongoing role that cost appears to play in the decision to use electronic surveillance, and the new structural privacy rights that appear to be developing. In the remainder of this section, I conclude by discussing some of the policy implications of this work.

First, my research suggests that commercial entities are not only playing a considerable role in criminal investigations, but they also appear to be exercising considerable discretion in how they fulfill this role. In a very real sense, commercial entities are exerting an influence over law enforcement investigations that has previously only been exerted by judges and legislatures. This raises considerable questions about how commercial entities decide how difficult it should be for law enforcement to obtain information, and whether commercial entities should continue to occupy this role. While one might expect concerns about public perceptions and financial repercussions to play a

significant role in how commercial entities decide to respond to commercial requests, these may not be the only concerns. Some companies may view themselves as protectors of their customer's privacy, and it may be useful for commercial entities to have an adversarial relationship with law enforcement, particularly if the customer himself is unaware of (and is never made aware of) law enforcement's request.

Indeed, there are significant benefits to entrusting companies to protect their customer's privacy against invasion by law enforcement officers. These companies may have extensive resources and expertise that they may be willing to use to protect their customer's interests, particularly if doing so is regarded as a sound business practice. Furthermore, these companies are likely to be repeat players who receive multiple requests from law enforcement, potentially reducing the cost of responding to requests. Large companies that receive many requests from law enforcement may even be able to observe and respond to trends, thus going beyond protecting particular individual's privacy to help enforce the balance of power between the individual and the state. For example, if a company perceives that law enforcement is requesting a particular form of information so frequently and with such little prior evidence that it may be tantamount to "unrestrained power to assemble data that reveals private aspects of identity" (*U.S. v. Jones*, 132 S. Ct. at 956 (2012)(Sotomayor, J., concurring)), the company may elect to increase the difficulty of obtaining the information.[43] Additionally, companies may help ensure predictability and uniformity across jurisdictions by refusing to turn over evidence unless law enforcement satisfies the higher showing of evidence required in some jurisdictions (Farivar 2013).

However, the role currently undertaken by commercial entities may not be ideal. Many of the tactics that commercial entities can use to limit law enforcement access to information are based on not necessarily tied to policy rationales for limiting law enforcement investigations. For example, a company that requires law enforcement information requests to specify the data type they are requesting in a highly technical way, and rejects any requests that do not fit this criterion, will release less information to law enforcement than a company that is more flexible. On the other hand, the requests that they do fill will not necessarily be those where law enforcement has a stronger basis for requesting information. Instead, requests are more likely to be filled when the requesting agency is technologically savvy enough to specify the right information type or has sufficient resources to make multiple requests. Although it is also true that law enforcement might be more likely to make repeated requests when they have stronger reason to believe that they will obtain incriminating evidence, the process of repeated

[43] Such a role would be in addition to the current role that private companies play in exposing surveillance trends by publishing data about the number and type of requests they receive from law enforcement (Google 2016).

requests burdens both law enforcement and the commercial entity responding to the request.

Additionally, reliance on commercial entities to regulate law enforcement access to customer information may lead to unpredictability and inequities from the point of view of the consumer. As companies vary in their responsiveness to law enforcement requests – and this variation is often hidden – consumers may be unable to either select companies that will be protective of their information or predict the conditions under which their information may be shared. Some companies may decide to make their privacy protecting practices well known by publicly objecting to some instances of law enforcement data collection;[44] however, without additional data it would be difficult to tell whether those objections represent general practices or outlier cases. More importantly, consumers may not be in a position to freely select companies that will provide higher level of protections for their data. Manufacturers that produce luxury goods may be more interested in protecting the privacy of their users; upscale markets may be served by multiple entities, allowing consumers to select the provide who is most protective of privacy. Relying on commercial entities to regulate law enforcement may retrench inequities that lead to over-policing of communities with lower socio-economic status.

Second, my research suggests that law enforcement considers different factors when deciding to use electronic surveillance and commercial information requests, which may suggest these categories of techniques should be regulated differently. In particular, information concerns – such as the quality and reliability of information – are much more of a concern in the context of commercial information requests than electronic surveillance. This raises an interesting question of what might happen if legal protections for commercial information requests are increased – for example, perhaps by requiring a warrant to obtain certain types of intimate or revealing commercial information. If commercial entities do not change their privacy protecting practices in response to the strengthening of legal protections, this may lead to overregulation of law enforcement and a suboptimal level of information collection. Legislators who are considering increasing legal protections for commercial information may want to pair those protections with increased regulation of how commercial entities respond to these requests, in order to avoid unintended consequences.

[44] For example, Apple's recent response to the FBI's request that they decrypt the San Bernardino shooter's phone could be seen as serving to publicly signal their interest in protecting the information of their customers. However, this point should not be overstated – signaling an interest in privacy is only one of many possible rationales for Apple's response in this instance.

4. The Gilded Age of Electronic Surveillance[45]

Abstract

While the Fourth Amendment is the primary source of Constitutional safeguards for individuals targeted by law enforcement surveillance, it has never been the only source of protection. Practical limitations on law enforcement's ability to collect information, including both technical and financial constraints, have long incentivized law enforcement officers to seek evidence of a crime prior to expending the resources necessary to conduct electronic surveillance. However, as technological improvements have reduced both the cost and difficulty of collecting information, these practical limitations are faltering. Judges are increasingly willing to consider the impact on practical limitations when deciding whether law enforcement use of a new surveillance technology constitutes a search, and is therefore worthy of Fourth Amendment protections.

Similarly, academics have extensively argued that changes in practical limitations can – and should – affect how the Fourth Amendment is interpreted. In particular, Professor Kerr has developed an "equilibrium-adjustment" theory of the Fourth Amendment, under which Fourth Amendment jurisprudence functions to ensure that law enforcement has a certain level of power to investigate crimes. When advances in technology make it easier for law enforcement to collect information, judges interpret the Fourth Amendment to enhance legal protections for individuals; when advances in technology make it easier for criminals to evade law enforcement surveillance, judges interpret the Fourth Amendment to ensure law enforcement faces fewer legal barriers to investigating crimes facilitated by the new technology. Further scholarship has analyzed when changes in technology have affected practical limitations to such an extent that the development of legal protections is warranted.

However, both the judiciary and academia have largely ignored a significant complication. There are over 12,000 local law enforcement agencies in the United States, and these agencies vary greatly in ways that may impact their ability to take advantage of changes in technology. In particular, large urban agencies may have the resources to develop specialized units that frequently use electronic surveillance, thus also developing personnel with significant expertise in using surveillance. On the other hand, personnel in smaller agencies may be less likely to specialize in areas that frequently use electronic surveillance, and thus may develop less surveillance expertise. Interpreting the Fourth Amendment to

[45] This work was funded by the James Q. Wilson Dissertation Fellowship at the Pardee RAND Graduate School. I would like to thank my Ed Balkovich, Sasha Romanosky, James Anderson, and Derek Bambauer for their valuable comments and feedback.

maintain a particular level of police power in large urban communities may undermine the ability of law enforcement officers in smaller communities to use electronic surveillance. Consequently, adopting equilibrium-adjustment theory or other similar rationales may lead to a gilded age of surveillance: an era in which some law enforcement agencies have extensive ability to conduct electronic surveillance, while others have little to no access to electronic surveillance.

In this article, I describe variation in local law enforcement agencies in the United States, and discuss how this variation may complicate attempts to address changes in practical protections against law enforcement surveillance. I begin by reviewing both the legal and practical protections against law enforcement surveillance. I pay particular attention to two recent trends that have undermined traditional practical protections against law enforcement surveillance: the decreasing cost of collecting information and the increasing availability of commercially collected data. I then discuss variation in the available resources and manpower across different types of law enforcement agencies that operate in the United States. I partition the agencies based on the size of the community they serve and, wherever possible, I quantitatively describe variation based on publicly available data from the Law Enforcement Management and Administrative Statistics (LEMAS) survey and the Uniform Crime Reporting (UCR) data.

I analyze how the variation I observe might affect the ability of law enforcement agencies to conduct electronic surveillance, and adapt to changes in technology. I conclude that there are several factors that may make it easier for law enforcement agencies that serve large communities to use electronic surveillance, when compared with law enforcement agencies that serve small communities. I then argue that failing to consider this variation when interpreting the Fourth Amendment in light of technological changes may create additional difficulties for smaller law enforcement agencies. I conclude by discussing ways that the Fourth Amendment protections could be crafted to account for declining practical protections, without stifling the ability of smaller agencies to adopt and employ electronic surveillance.

The Fourth Amendment has long been the primary source of Constitutional safeguards for individuals targeted by law enforcement surveillance. This Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[46] Consequently, law enforcement must obtain a warrant or find an exception to the warrant clause before conducting a search of a home,[47] planting a GPS tracker on a car,[48] or accessing the contents of an individual's cell phone.[49]

Technology has changed how law enforcement officers conduct criminal investigations – for better or worse. The Fourth Amendment was written in a world where law enforcement faced many barriers to collecting information about individuals. To collect information about communications, they could only listen in on conversations,[50] rely on informants,[51] or obtain and open an individual's letters.[52] To collect information about location, they could only physically follow a suspect.[53] And even when surveillance was possible, it was often extraordinarily expensive.[54] Recent Fourth Amendment literature has described these barriers as creating practical protections for individual privacy.[55] As a matter of law, police had wide latitude to obtain information about individuals; as a matter of practice, police faced such stark difficulties in obtaining this information that they would only invest effort in doing so when they believed the results would be crucially important in a serious criminal investigation.[56]

The world has since moved on. Law enforcement can now obtain communications information by listening in on phone calls,[57] intercepting text messages,[58] and reading email;[59]

---

[46] U.S. Const. amend. IV (1791).

[47] *Payton v. New York*, 445 U.S. 573 (1980).

[48] *U.S. v. Jones*, 132 S.Ct. 945 (2012).

[49] *Riley v. California*, 134 S.Ct. 2473 (2014).

[50] Without technological assistance, listening in on conversations is difficult and required close proximity to the speakers. For example, the word "eavesdropping" originally referred to the space under the overhang of a roof; it eventually came to be used to describe intentionally overhearing a conversation because a person would need to stand that close to a house in order to hear to occupants' conversations within. Merriam-Webster, *Words at Play: Eavesdrop, Fiasco, and 8 More Words with Surprising Origins*, http://www.merriam-webster.com/words-at-play/top-10-words-with-remarkable-origins-vol-1/eavesdrop (last visited Sept. 15, 2016).

[51] *Hoffa v. United States*, 385 U.S. 293 (1966).

[52] Daniel J. Solove, *A Brief History of Information Privacy Law*, 1-7, ttp://papers.ssrn.com/sol3/papers.cfm?abstract_id=914271.

[53] Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of* United States v. Jones, 123 Yale L. J. 335 (2014).

[54] *Id.*

[55] Harry Surden, *Structural Rights in Privacy*, 60 S.M.U. L. Rev. 1605, 1612 (2007).

[56] Surden, *supra* note 55.

[57] Law enforcement has had the ability to intercept phone calls using wiretaps since at least the 1890s. Samuel Dash, *The Eavesdroppers* 25 (1959).

[58] *Ontario v. Quon*, 130 S.Ct. 2619 (2010).

they can obtain location information using GPS trackers[60] and cell site location data.[61] As a result of these technological changes, the practical barriers that once served as the primary protection for privacy have been severely compromised.[62] Law enforcement now has many methods for obtaining information quickly and cheaply. In addition, law enforcement departments are no longer the only type of entity seeking information about individuals. Commercial firms now collect, store, and analyze tremendous amounts of information about their customers, information that may be available to law enforcement with minimal legal process.

Judges and scholars alike have labored to interpret the Fourth Amendment in light of these tectonic technological shifts in law enforcement's ability to obtain information.[63] One recent trend amongst both judges and academics has been to explicitly discuss how a new form of technology has reduced practical barriers to law enforcement surveillance, often by making surveillance cheaper and more technically feasible. In *United States v. Jones*, Justice Alito noted in a concurring opinion that, before the advent of GPS technology, constant monitoring of a suspect was so expensive that "[o]nly an investigation of unusual importance could have justified such an expenditure of law enforcement resources."[64] Several scholars have gone further, attempting to derive a standard that can be used to determine whether improvements in technology have reduced practical protections to the point that further legal protections may be warranted. For example, one scholar has "arrive[d] at a rough rule of thumb: If the cost of the surveillance using the new technique is an order of magnitude (ten times) less than the cost of the surveillance without using the new technique, then the new technique violates a reasonable expectation of privacy" and consequently should be subject to Fourth Amendment protections.[65]

However, there is a foundational issue that must be resolved before attempting to restore a balance of power between the individual and the state. As of 2013, there were 12,000 local law enforcement agencies in the United States,[66] in addition to numerous state and federal agencies. These agencies vary greatly in many characteristics that may affect their ability to take advantage

---

[59] *United States v. Warshak*, 631 F.3d 266 (2010).

[60] *United States v. Jones*, 132 S.Ct. 945, 948 (2012).

[61] *State v. Earls*, 70 A.3d 630 (2013).

[62] Surden, *supra* note 55.

[63] The difficulties in fitting jurisprudence from one era with the realities of another have resulted in doctrine that has been described as "an embarrassment." Akhil Reed Amar, *Fourth Amendment First Principles*, 107 Harv. L. Rev. 757, 757-8 (1994) ("[P]illars of modern Fourth Amendment case law are hard to support; in fact, today's Supreme Court does not really support them. Except when it does….Meanwhile, sensible rules the Amendment clearly does lay down or presuppose…are ignored by the Justices. Sometimes. The result is a vast jumble of judicial pronouncements that is not merely complex and contradictory, but often perverse.").

[64] *United States v. Jones*, 132 S.Ct. 945, 964 (2012).

[65] Bankston and Soltani, *supra* note 53 at 351 (2014).

[66] Bureau of Justice Statistics, *Local Police*, http://www.bjs.gov/index.cfm?ty=tp&tid=71.

of new surveillance technologies, including available resources, manpower capacity and capabilities, organizational structure, and situational factors. This variation is particularly stark between agencies that serve large, urban communities and agencies that serve small, rural communities. Police officers operating in Washington D.C.[67] face fundamentally different constraints than those officers operating in Washington, Pennsylvania.[68] Technological changes can – and frequently do – affect the balance of power between police power and individual privacy in urban jurisdictions without similarly affecting small communities. If the Fourth Amendment is interpreted to correct an imbalance of between police power and individual privacy in large jurisdictions created by changes in technology, this interpretation may simultaneously undermine the existing balance of power in communities where law enforcement agencies are less able to take advantage of technological changes.

In this paper, I argue that efforts to interpret the Fourth Amendment to restore the balance between police power and individual privacy in light of technological changes must account for variation in law enforcement capabilities across different types of jurisdictions – particularly variation across law enforcement agencies serving different sized communities. If this variation is not considered, we run the risk of turning the golden age of surveillance into the gilded age[69] of surveillance: a scenario where a certain strata of law enforcement agencies has extensive capacity to engage in electronic surveillance, while other departments have very limited electronic surveillance capacity.

I begin by describing both the legal and practical limitations on law enforcement surveillance. Next, I describe variation across different local law enforcement agencies in the United States, focusing particularly on differences in factors that are thought to affect law enforcement decision making. Then, I discuss how this variation interacts with the technological trends described in the previous section, leading to differential abilities to take advantage of improvements in technology, and analyze how attempting to correct the imbalance in police power and individual privacy in large communities could in fact create or exacerbate imbalance in smaller communities. Finally, I describe potential alternatives for interpreting the Fourth Amendment in light of law enforcement variation.

---

[67] As of 2015, the District of Columbia has an estimated population of 672,228. *QuickFacts: District of Columbia*, U.S. Census Bureau, http://www.census.gov/quickfacts/table/PST045215/11.

[68] As of 2014, Washington, Pennsylvania has a population of 13,551. *Washington, Pennsylvania*, http://www.city-data.com/city/Washington-Pennsylvania.html

[69] The United States in the late nineteenth century is frequently referred to as in a "Gilded age" where there were "large inequalities of wealth, which undermined the existing legal system." Edward Glaeser, Jose Scheinkman, and Andrei Shleifer, *The injustice of inequality*, 50 J. Monetary Econ. 199, 201 (2003).

I. Regulation of Law Enforcement Searches

A. Legal Limitations

The primary constitutional restraint on law enforcement searches is the Fourth Amendment, which protects "persons, houses, papers, and effects against unreasonable searches and seizures."[70] Written in response to the use of generalized warrants by the British government prior to the Revolutionary War,[71] this amendment was intended to restrain invasive government actions while still allowing law enforcement to investigate crimes and protect public safety.[72] These parallel goals still underlie interpretation of the Fourth Amendment in modern times.

The Fourth Amendment was initially interpreted to restrict government actors to the same extent that trespass law restricted private actors. If a particular search would require that law enforcement commit an act that would be a common law trespass if committed by a private actor, then this action was forbidden by the Fourth Amendment, absent judicial permission or a similar exception to the warrant requirement.[73] For example, in *Olmstead v. United States*, the Supreme Court utilized the trespass theory of the Fourth Amendment to hold that Fourth Amendment protections did not apply to law enforcement use of wiretaps to intercept telephone communications.[74] Since the wiretapping could be accomplished without physical intrusion onto the defendant's property, the majority opinion held that the Fourth Amendment did not apply.[75] "The language of the Amendment can not be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office."[76]

Justice Brandeis filed a vociferous and often-cited dissent, in which he expressed concern that future changes in technology might largely undermine Fourth Amendment protections.[77] Since "[w]ays may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court," Justice Brandeis argued that Fourth

---

[70] U.S. Const. Amend. IV.

[71] David E. Steinberg, *The Uses and Misuses of Fourth Amendment History*, 10 U. Pa. J. Const. L. 581, 585 (2008).

[72] However, there is significant disagreement between scholars about the history of the Fourth Amendment. *See*, *e.g.*, Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 Ind. L.J. 979, 983-989 (2011) (describing "two fundamentally opposed views about the history and original purpose of the Fourth Amendment").

[73] *Olmstead v. United States*, 277 U.S. 438 (1928).

[74] *Id.* at 466.

[75] *Id.* at 465 ("The language of the Amendment can not be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office any more than the highways along which they are stretched.").

[76] *Id.* at 465.

[77] *Id.* at 469.

Amendment protections should not only apply when a physical invasion of the home occurred.[78] Brandeis specifically voiced concerns about how changes in technology made it easier for law enforcement to obtain evidence. While torture and trespass were the "simple evils" known to the writers of the Fourth and Fifth Amendments,[79] "[d]iscovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet."[80]

The Supreme Court has since fundamentally altered its approach to the Fourth Amendment. In *Katz v. United States*, the Supreme Court explicitly overruled *Olmstead*. As was articulated by in Harlan's concurring opinion, and subsequently adopted by the Supreme Court in *Smith v. Maryland*,[81] Fourth Amendment protections apply whenever a "twofold" requirement" is satisfied: "first, that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[82] Under this new approach, the Court in *Katz* held that the attachment of an electronic recording device to the outside of a telephone booth constituted a search, because "[t]he Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied."[83] Since then, the Supreme Court has clarified that the reasonable expectation of privacy standard did not eliminate the trespass approach to the Fourth Amendment; rather, physical invasion by law enforcement onto private property would be governed by the trespass approach, while law enforcement actions that did not physically intrude onto a protected space would be governed by the reasonable expectation of privacy standard.[84]

---

[78] *Id.* at 474.

[79] *Id.* at 474 ("When the Fourth and Fifth Amendments were adopted, 'the form that evil had theretofore taken,' had been necessarily simple. Force and violence were then the only means known to man by which a Government could directly effect self-incrimination. It could compel the individual to testify – a compulsion effected, if need be, by torture. It could secure possession of his papers and other articles incident to his private life – a seizure effected, if need be, by breaking and entry.").

[80] *Id.* at 474.

[81] *Smith v. Maryland*, 442 U.S. 735, 740 (1979).

[82] *Katz v. United States*, 389 U.S. 347, 361 (1967). As a practical matter, the reasonable expectations of privacy defined in the cases that followed *Katz* were often coextensive with property rights. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801 (2004).

[83] *Id.* at 353.

[84] *United States v. Jones*, 132 S. Ct. 945, 953 (2012) ("What we apply is an 18th-century guarantee against unreasonable searches, which we believe must provide *at a minimum* the degree of protection it afforded when it was adopted….[W]e do not make trespass the exclusive test. Situations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis.")

Subsequent case law has refined the reasonable expectation of privacy standard in important ways. For example, the development of the third party doctrine has significantly limited Fourth Amendment protections in communication and business records.[85] Originally articulated in *United States v. Miller*, the third party doctrine maintains 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 only be used for a limited purpose and the confidence placed in the third party will not be betrayed."[86] Under this doctrine, an individual has no Fourth Amendment interests in information that is shared with a service provider in the ordinary course of using a consumer device.[87]

The increase in the amount of information individuals share with commercial service providers during the ordinary activities of daily living has made the third party doctrine a major gap in Fourth Amendment protections. That said, not all information that has been transmitted to a third party is available to law enforcement without a warrant, as other principles about what information is private come into play. In particular, the contents of private communications are likely to be protected by the Fourth Amendment.[88] For example, federal law enforcement once argued that provisions of the Stored Communications Act that allow them to access emails in storage over 180 days were constitutional.[89] However, the Sixth Circuit held that "it is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment", despite the fact that the ISP may be able to access the contents of the communication.[90] While this was only a circuit court opinion, it has had a wide-ranging and enduring impact, particularly as certain commercial services providers have used its rule to justify requiring a warrant before turning over information in any jurisdiction.[91]

The application of the Fourth Amendment to emerging technologies has provoked much controversy, particularly as analogies between traditional and emerging sources of information often fall flat. Since the turn of the century, courts and scholars have analyzed the Fourth

---

[85] *United States v. Miller*, 425 U.S. 435 (1976).

[86] *Id.* at 443. However, individuals may still maintain a privacy interest in the content of their communications, even if they have been transmitted through a third party service provider. *See U.S. v. Warshak*, 631 F.3d 266 (2010).

[87] *See Smith v. Maryland*, 442 U.S. 735 (1979).

[88] *See* Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 Wm. & Mary L. Rev. 2105 (2009).

[89] *See U.S. v. Warshak*, 631 F.3d 266 (6th Cir 2010), vacated in part on other grounds, 532 F.3d 521, 18 U.S.C. § 2703.

[90] *Id.* at 286-7

[91] Cyrus Farivar, *Google stands up for Gmail users, requires cops to get a warrant*, Ars Technica (Jan 23. 2013), *available at* http://arstechnica.com/tech-policy/2013/01/google-stands-up-for-gmail-users-requires-cops-to-get-a-warrant/

Amendment effects of, among others, thermal imaging,[92] biometrics,[93] cell site location information,[94] and GPS tracking technology.[95] These analyses have formed an extensive and growing literature on how emerging technologies lower the practical privacy protections that have traditionally limited law enforcement surveillance – as well as whether and how legal privacy protections should be extended to cover this gap.

B. Practical Limitations

Although practical limitations[96] have always played a significant role in the regulation of law enforcement searches, this role has only become conspicuous by its absence. It is only in recent years that this function has been recognized, as technological improvements in both consumer devices and surveillance equipment have enabled law enforcement to collect increasingly intimate information with decreasingly onerous outlay of resources. As technology has made it easier for government officers to obtain information about criminal suspects, judges, scholars, and privacy advocates have turned their attention to whether and how Fourth Amendment rights should change in the face of these new technologies. These analyses begin from the proposition that "many privacy interests are protected not by positive legal prohibitions on behavior, but by structural constraints which act as reliable substitutes for legal constraints."[97] Technological improvements have decreased the non-legal constraints limiting law enforcement access to surveillance, by making data collection cheaper[98] and more technically feasible.[99]

---

[92] *See*, *e.g.*, *Kyllo v. United States*, 533 U.S. 27 (2001), Note, *The Fourth Amendment and New Technologies: The Constitutionality of Thermal Imaging*, 46 Vill. L. Rev. 241 (2001).

[93] *See*, *e.g.*, Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 Tex. L. Rev. 1349 (2004).

[94] *See*, *e.g.*, *Commonwealth v. Augustine*, 4 N.E. 3d 846 (Mass. 2014), Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 60 Maryland L. Rev. 677 (2011).

[95] *See*, *e.g.*, *U.S. v. Jones*, *supra* note 60, Renee McDonald Hutchins, *Tied Up in Knotts? GPS Technology and the Fourth Amendment*, 55 UCLA L. Rev. 409 (2007).

[96] These limitations include both financial cost and technical difficulty of obtaining information. In this paper, I refer to these constraints as "practical limitations", adopting the terminology used by Justice Alito in *United States v. Jones*. 132 S.Ct. 945, 963 ("In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical.").

[97] Harry Surden, *Structural Rights in Privacy*, 60 S.M.U. L. Rev. 1605, 1612 (2007).

[98] *See generally*, Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of* United States v. Jones, 123 Yale L. J. 335 (2014).

[99] See, e.g., Peter Swire and Kenesa Ahmad, *Encryption and Globalization*, 13 Colum. Sci. & Tech L. Rev. 416, 470 (2012) (arguing that technological changes have created a "'golden age for surveillance' because investigatory agencies have unprecedented access to information about a suspect" and "data mining provides new tools for identifying suspects and their contacts").

On their face, technological improvements that make it easier for law enforcement to investigate criminal activity would appear to be societally beneficial: law enforcement could spend the resources saved on other investigations, or society can redistribute the money allocated to law enforcement. However, judges, scholars, and advocates have all expressed concern that, as surveillance methods are developed which all law enforcement to more easily collect information about an individual, law enforcement will require less preliminary evidence of an individuals' guilt before employing these methods. Technological innovations that make it easier for law enforcement to collect information may therefore increase the likelihood that an innocent individual will be subjected to police surveillance, potentially injuring their privacy and dignity.[100] Additionally, improvements in technology could undermine traditionally existing practical protections against law enforcement surveillance, thus allowing law enforcement to conduct more extensive and intrusive surveillance.

In order to maintain the allocation of power between the individual and the state underlying much of Fourth Amendment jurisprudence, scholars have argued that courts can – and should – respond to changes in technology that make it easier for law enforcement to obtain information about individuals by increasing the legal protections that apply to this information. Kerr attributes these responses to an "equilibrium-adjustment" dynamic underlying Fourth Amendment jurisprudence.[101] This theory claims that "judges respond to new facts in Fourth Amendment law in a specific way: judges adjust Fourth Amendment protection to restore the preexisting level of police power."[102] Consequently, when technological innovations make it easier and cheaper for law enforcement to conduct surveillance, judges respond by increasing legal protections to maintain the balance of power between the individual and the state.[103]

Although no court has explicitly adopted the equilibrium-adjustment framework, courts frequently acknowledge that part of their goal in interpreting the Fourth Amendment is to maintain a balance between individual privacy and public safety. According to the Wisconsin Supreme Court, "[t]he Fourth Amendment often conjures the image of a scale on which we balance the needs of law enforcement and the rights of individuals," and "[t]echnological innovation does not change the need for balance."[104] Similarly, the California Supreme Court

---

[100] *Cf.* Jane Bambauer, *Hassle*, 113 Mich. L. Rev. 461, 465 (2015) (coining the term "hassle" to describe "the probability that an innocent person within the relevant population will be stopped or searched" under a particular surveillance protocol and suggesting that accounting for hassle may help ensure that the social costs of surveillance are justified).

[101] *See generally* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 Harv. L. Rev. 476 (2011).

[102] *Id.* at 487.

[103] *Id.* at 489.

[104] *State v. Subdiaz-Osorio*, 849 N.W.2d 748, 761 (Wis. 2014). The court went on to explain the difficulty of maintaining this balance. "It is no small task to afford law enforcement officers

describes Constitutionally permissible rules for police conduct as "strik[ing] a balance between a person's interest in immunity from police interference and the community's interest in law enforcement."[105]

Acknowledging the need to balance privacy and security does not imply that judges should seek to preserve any particular balance. To demonstrate the later point, Kerr provides six categories of situations where the Supreme Court interpreted the Fourth Amendment to restore a hypothetical balance of power between the individual and the state that would have existed absent technological developments.[106] Kerr supports these categories with numerous descriptions of specific cases where the Supreme Court acted to restore the balance of power that existed before technological development. For example, when law enforcement develops new methods of obtaining information that was previously unavailable to them without a warrant, the judiciary interprets the Fourth Amendment broadly to require law enforcement to obtain a warrant before using those methods. Therefore, in *Kyllo v. United States*,[107] the Court was "confronted with a new technological tool that threatened 'to erode the privacy guaranteed by the Fourth Amendment'", and "interpreted the Fourth Amendment in a way that 'assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"[108] Similarly, the Supreme Court's decisions in *Knotts*[109] and *Karo*[110] can be explained as "preserv[ing] the same basic set of police powers with beepers that the police had without them": law enforcement can monitor activity that takes place in public without a warrant, but must obtain a warrant before seeking information about activity conducted in a private residence.[111]

---

and government agencies the leeway they need to keep citizens safe while ensuring that citizens retain a reasonable degree of privacy." *Id.*

[105] *People v. Mickelson*, 59 Cal. 2d 448, 452 (Cal. 1693).

[106] Kerr, *supra* note 101, at 494-525.

[107] In *Kyllo v. United States*, the Supreme Court determined that "the use of a thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within the home constitutes a 'search' within the meaning of the Fourth Amendment." *Kyllo v. United States*, 533 U.S. 27, 29 (2001).

[108] Kerr, supra note 101, at 498. *But see* Stephanie M. Stern, *The Inviolate Home: Housing Exceptionalism in the Fourth Amendment*, 95 Cornell L. Rev. 905 (2010) (criticizing the focus on the home in Fourth Amendment jurisprudence and scholarship).

[109] In *Knotts*, the Supreme Court held that the use of a radio transmitter to track a suspect's car on public streets does not constitute a search for purposes of the Fourth Amendment, where the information obtained through the transmitter could have also been obtained through visual surveillance. *United States v. Knotts*, 460 U.S. 276 (1983).

[110] In *Karo*, the Supreme Court held that the use of a radio transmitter to obtain information about activity conducted inside a private residence constituted a search for purposes of the Fourth Amendment. *United States v. Karo*, 468 U.S. 705 (1984).

[111] Kerr, *supra* note 101, at 500.

However, when criminals develop new tools that allow them to conduct criminal activity more easily, the Fourth Amendment is interpreted narrowly such that law enforcement can easily investigate these tools. Kerr uses this principal to justify the weak Fourth Amendment protections applied in the context of automobile searches.[112] Even though stopping and going-over a car is considered a seizure and a search for purposes of the Fourth Amendment, a warrant is not required for either action. Instead, because of the car's inherently mobile nature, "the judgment of the police as to probable cause serves as a sufficient authorization for a search."[113] Kerr explains the Supreme Court's car jurisprudence as a response to the car as a technological development. At the time the automobile was first developed and popularized, the public was greatly concerned that it could be used to facilitate criminal activity, particularly bootlegging. As Kerr explains, the modest level of privacy protection for the search and seizure of cars counterbalances the benefits that automobiles otherwise offer to criminals who use them to hide evidence of crime."[114]

In addition to explaining how the Fourth Amendment developed in the past, equilibrium-adjustment theory has great potential to explain how the Fourth Amendment could be –and should be – interpreted in light of emerging technologies. However, there are several difficulties inherent in determining when technology has evolved to the point that further legal protections are warranted. In the remainder of this section, I describe two areas of technological development that are currently threatening practical protections against law enforcement searches: the declining cost of surveillance and increasing availability of commercially collected consumer data. While these trends are not exhaustive – nor entirely mutually exclusive[115] – they represent significant and important ways that technology can erode practical privacy protections. I then describe how judges and scholars have recognized and reacted to the trend. As will be seen, while there is consensus that further legal protections may be warranted in some circumstances, the proposed standards for determining when these legal protections are necessary may not account for important variation in law enforcement agencies.

---

[112] Kerr, *supra* note 101, at 502.

[113] *Chambers v. Maroney*, 399 U.S. 42, 51 (1970). "[A] search warrant [is] unnecessary where there is probable cause to search an automobile stopped on the highway; the car is movable, the occupants are alerted, and the car's contents may never be found again if a warrant must be obtained." *Id.*

[114] Kerr, *supra* note 101, at 503.

[115] For example, commercial collection of data lowers the cost to law enforcement of obtaining certain types of information, since law enforcement can rely on data collected by commercial entities more cheaply than collecting data on their own. However, despite this overlap, each trend has had a distinct effect on law enforcement surveillance and, as will be discussed later, may be expected to affect different types of law enforcement agencies differently. *See supra* section IV.

1. Technological Trends that Reduce Practical Protections on Surveillance

a. Reduction in cost

Technological improvements in both consumer devices and law enforcement surveillance tools have created new, lower-cost methods for law enforcement to obtain information during criminal investigations.[116] There are different types of costs, which may affect law enforcement decision making in different ways. Marginal costs, which are the costs incurred in utilizing an additional "unit" of electronic surveillance,[117] scale with the amount of surveillance used. For example, if it costs a law enforcement agency $105 to use a cell-site simulator[118] to track a suspect's location for an hour, then it probably costs that same agency approximately $210 to use the same device to track the suspect's location for two hours.[119]

On the other hand, fixed costs, which are the cost incurred in developing the capacity to use electronic surveillance,[120] do not scale with the amount of surveillance used. Instead, these costs are the same regardless of how often a law enforcement agency elects to use a particular form of electronic surveillance. For example, before a law enforcement agency can use a cell-site simulator to track a suspect's location, they must first procure this device, either by purchasing or borrowing it.[121] The cost of purchasing or borrowing this device must be incurred in order to

---

[116] *See generally*, Bankston and Soltani, *supra* note 53.

[117] In the economics literature, marginal costs are most often discussed in the context of defining the cost of producing an additional unit of product to a firm that is already engaged in producing that product. Under those circumstances, "[t]he marginal cost of an additional unit of output is the cost of the additional inputs needed to produce that output. EconModel, *Marginal Cost (MC), available at* http://www.econmodel.com/classic/terms/mc.htm.

[118] A Stingray device "deceives nearby cell phones into believing that the device is a cell tower so that the cell phone's information is then downloaded into the cell site simulator." Brian L. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 Hastings L. J. 183, 185 (2014). They can be used to track a suspect's location by determining the signal strength of his cell phone from several different spots, and then using that information to triangulate his location. *Id*. at 193.

[119] In *Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones*, Bankston and Soltani estimate the marginal cost of tracking a suspect's location using various forms of physical and electronic surveillance. They conclude that it would cost approximately $105 to track a suspect's location using a Stingray. Bankston and Soltani, *supra* note 53, at 350.

[120] "A fixed cost is a cost that remains unchanged in total, regardless of changes in the level of total activity or volume. *Fixed/Variable Cost*, http://kwhs.wharton.upenn.edu/term/fixed_variable-cost/. Recalling the example of the firm producing a product discussed in footnote 117, a fixed cost would be the cost of purchasing the factor that manufactures the product.

[121] As of 2013, the latest edition of a Stingray device cost approximately $134,952. Ryan Gallagher, *Meet the machines that steal your phone's data*, Ars Technica (Sept. 25, 2013),

develop the capacity to use this form of electronic surveillance, regardless of how often it is used.

To demonstrate how these different types of costs may affect law enforcement decision making, consider two scenarios: one in which electronic surveillance allows collection of information with both low marginal and low fixed costs, and one in which electronic surveillance allows collection of information with low marginal costs but high fixed costs.[122] If a new form of electronic surveillance allows law enforcement to obtain a particular type of information with low marginal costs and low fixed costs, then there are few financial barriers faced by law enforcement agencies that wish to use this form of surveillance. Under these circumstances, all law enforcement agencies will be able to use this form of surveillance, subject to their ability to pay the low cost required.

However, if a new form of electronic surveillance allows law enforcement to obtain a particular type of information with low marginal costs but high fixed costs, then the financial barriers faced by law enforcement agencies that wish to use this form of surveillance resemble a step function. There is a steep financial barrier that must be surmounted before this form of electronic surveillance can be used at all. However, once this threshold has been reached, then the cost of using the surveillance in additional cases is small and therefore there are few additional financial barriers. In this instance, cost serves not as a limitation on the amount of surveillance an agency can use, but as a differentiator between agencies that can use this surveillance at all.

There are strategies a smaller law enforcement department could use to overcome the barriers created by the high fixed cost of using a particular form of surveillance. They may be able to borrow or lease equipment from other agencies. For example, Texas has a centralized system for conducting communications interceptions.[123] However, relying on an outside agency to assist in surveillance creates its own set of barriers. The outside agency may also be responsible for assisting other localities, requiring sharing of finite resources. Continuing the example from Texas, as of 2009 the Texas Department of Public Safety "has four rooms for monitoring and recording wiretaps", each with the capacity to monitor two phone lines.[124] This creates a natural ceiling on the number of communications intercepts that can occur in Texas at one time.

---

available at http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/.

[122] Because high marginal costs impose the type of privacy-protecting barriers that have traditionally limited law enforcement searches (regardless of whether fixed costs are high or low), I omit these situations from this analysis.

[123] "The Texas Department of Public Safety (DPS) is the only agency authorized to possess, install, and operate wiretapping equipment pursuant to State law." Jeff Strange, *A primer on wiretaps, pen registers, and trap and trace devices*, 39 Texas District & County Attorneys Association (2009), *available at* http://www.tdcaa.com/node/4813.

[124] *Id.*

b. Increase in commercial collection of data

In recent years, an entire industry has sprung up around finding new ways to harvest, compile, and analyze consumer data, creating information that can be used by advertisers, consumer products manufacturers, and other businesses to reach out to consumers more effectively.[125] Information collected by commercial entities can be valuable to law enforcement as well, particularly as Fourth Amendment protections do not apply.[126] Law enforcement use of commercial data is not a new phenomenon; in particular, bank records[127] and phone records[128] have been used by law enforcement for decades. What is new, however, is the breadth of consumer devices that collect information, and the depth of information that they collect. For example, cell phones location information can be used to tell whether a suspect was at the scene of a crime;[129] Fitbits and other wearables can be used to determine whether a person's physical activity level matches their testimony;[130] Netflix and other streaming entertainment services can be used to determine whether a suspect has fled the country.[131]

The near-ubiquity of commercial data collection allows law enforcement to obtain information about a suspect at much lower cost than via traditional methods of surveillance.[132] Law enforcement can use information collected by commercial entities at both low fixed and low variable cost, suggesting that officers face few if any financial barriers to employing this mode of surveillance. While statutory law does require that law enforcement reimburse commercial

---

[125] For example, one way this information is used is to craft personalized recommendations to "help[] selective customers find which products they would like to purchase." Jae Keyong Kim, Yoon Ho Cho, *et al.*, *A personalized recommendation procedure for Internet shopping support*, 1 Electronic Commerce Research and Applications 301, 305 (2002).

[126] *See* discussion of the third party doctrine, *supra* section I.A.

[127] *United States v. Miller*, *supra* note 85, was decided in 1976 and concerned law enforcement access to bank records.

[128] *Smith v. Maryland*, *supra* note 87, was decided in 1979 and concerned law enforcement access to phone records.

[129] Robinson Meyer, *Do Police Need a Warrant to See Where a Phone Is?*, The Atlantic (Aug. 8, 2015), *available at* *http://www.theatlantic.com/technology/archive/2015/08/warrantless-cell-phone-location-tracking/400775/.*

[130] Mariella Moon, *Fitbit tracking data comes up in another court case*, Engadget (June 18, 2015), *available at* http://www.engadget.com/2015/06/28/fitbit-data-used-by-police.

[131] Tim Cushing, *Meet Your Newest Law Enforcement Partners: Netflix and Spotify*, Techdirt (Jul. 13, 2015), *available at* https://www.techdirt.com/articles/20150710/11442531614/meet-your-newest-law-enforcement-partners-netflix-spotify.shtml

[132] For example, Bankston and Soltani estimate that law enforcement can use cell phone location information to track a suspect for as little as $1.25/hour, while having an officer follow the suspect around would cost approximately $50/hour (or $250/hour if the surveillance was covert). Bankston and Soltani, *supra* note 53, at 350.

entities for the expense required to compile and report the information, these costs are generally lower than the costs that would be incurred if law enforcement collected the data directly.[133]

However, commercial collection of data does more than just lower the cost of obtaining information about a suspect. While law enforcement officers target their data collection to people and situations where they believe a crime has occurred or is likely to occur, commercial entities collect data frequently and target all information they consider to be economically advantageous. Consequently, commercial entities are much more likely than law enforcement to collect information before and during an unanticipated criminal act, such as a spontaneous crime or an unforeseen act of terrorism. This commercially collected information can be extremely valuable. For example, the Federal Bureau of Investigation was recently willing to pay over a million dollars to obtain access to the information contained on the San Bernardino shooter's smartphone, suggesting that they saw great benefit in obtaining this information.[134]

Commercial data collection greatly lowers the practical limitations protecting individual privacy against government surveillance. Law enforcement can obtain information at low cost, and are not limited to data collected after they are aware a criminal act has occurred. Nevertheless, barriers to law enforcement use of commercial collected data do exist. First, law enforcement must be aware the data is being collected, and where they can go to obtain the data. While these questions seem simple in theory, in practice constant changes in both technology and commercial relationships can make it difficult to find answers.[135]

Second, once the appropriate commercial entity has been located, law enforcement must successfully obtain the information from the commercial entity – generally without alerting the target of the investigation to their request. However, commercial entities may require specific technical information in order to comply with a law enforcement request for information, and it may be difficult for law enforcement to anticipate what technical information may be required in each case.[136] This can lead to a back-and-forth negotiation with the commercial entity that

---

[133] *See*, *e.g.*, Bankston and Soltani, *supra* note 53 at 350. However, the cost of obtaining information may vary from company-to-company, and can increase if law enforcement's request is broad or does not align with the way the commercial entity stores their data. *See* discussion *infra*.

[134] Wesley Bruer, *FBI paid more than $1 million to hack San Bernardino shooter's iPhone, Comey says*, CNN (Apr. 21, 2016), *available at* http://www.cnn.com/2016/04/21/politics/san-bernardino-iphone-apple-hacking/. This is not to say that the information gathered from the cell phone was necessarily worth the price paid for it; but rather that the price the FBI was willing to pay suggests that they expected the information found to be of significant value to criminal investigations.

[135] *See* Edward Balkovich, Don Prosnitz *et al*., *Electronic Surveillance of Mobile Devices*, RAND Report RR800 (2015), *available at* http://www.rand.org/pubs/research_reports/RR800.html.

[136] *Reconsidering Law Enforcement Use of Electronic Surveillance: Dollars and Sense* ("As one officer interviewed noted 'I don't think we can expect your average police officer to

consumes investigative time and resources."[137] Additionally, several social media companies have objected to court orders, particularly where they are required to release their customer's information without notice.[138]

2. Judicial Reactions

Courts have increasingly recognized that reducing barriers to surveillance use may undermine traditionally available practical protections for privacy. In *United States v. Jones*, the Supreme Court recently addressed the constitutionality of using a GPS tracker to continuously trace a suspect's location for 28 days.[139] While the majority opinion in *Jones* determined that a search had occurred under a trespass framework,[140] five justices signed onto concurring opinions finding a search had occurred under alternative rationales. Justice Alito, along with Justices Ginsburgh, Breyer, and Kagan, adopted the reasonable expectation of privacy test as the sole test for determining whether a search had occurred. Justice Alito noted in his concurrence that continuous location monitoring without electronic surveillance "was difficult and costly" and therefore "[o]nly an investigation of unusual importance could have justified such an expenditure

---

understand the difference between an IMEI and an IMSI. You know, you can't ask them what the IP for your computer is, or your internet provider…Most of us don't know those things. Most of us aren't going to know exactly what to ask for in a Facebook warrant.'")

[137] *Id.* ("According to one officer interviewed, the commercial entity 'might call back and say, 'Oh, you didn't ask for the right thing. You're getting nothing. Resubmit a new warrant or a new thing, a new request.'")

[138] Alex Fitzpatrick, *Twitter fights court order for user's data.* CNN.com (May 9, 2012), *available at* http://www.cnn.com/2012/05/09/tech/social-media/twitter-court-order. Objections to government requests for information are not new; however, the laws requiring certain types of companies to turn over certain types of information have been well settled for decades. For example, the Supreme Court held that phone companies could be required to assist law enforcement agencies install pen registers in 1977. *United States v. New York Telephone Co.*, 434 U.S. 159 (1977). Furthermore, Congress passed the Communications Assistance for Law Enforcement Act in 1994, expanding the amount of technical assistance that could be required of telecoms. *See* Federal Communications Commission, *Communications Assistance for Law Enforcement Act*, https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance.

[139] *United States. v. Jones*, 132 S. Ct. 945 (2012).

[140] In other words, a search had occurred because the police had physically planted the GPS tracker under the suspect's car, which was a trespass and therefore would have been considered a search at the time the Fourth Amendment was written. *United States v. Jones*, 132 S. Ct. at 949 ("It is important to be clear about what happened in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.").

of law enforcement resources."[141] However, GPS tracking devices "make long-term monitoring relatively easy and cheap," therefore reducing the privacy protections created by practical barriers to law enforcement use of surveillance.[142] Justice Alito specifically mentioned that "the best solution to privacy concerns may be legislative" as these decision makers are capable of, among other things, "balanc[ing] privacy and public safety in a comprehensive way."[143] In the absence of such legislative action, however, the Court must find that long-term GPS monitoring may violate a reasonable expectation of privacy as "society's expectation has been that law enforcement agents and others would not – and indeed, in the main, simply could not – secretly monitor and catalogue every single movement of an individual's car for a very long period."[144]

Justice Sotomayor, who also signed onto the majority opinion, wrote a separate concurrence. She did not reach the issue of whether use of whether GPS monitoring absent physical intrusion on private property constitutes a search,[145] but noted that "GPS monitoring – by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, choses to track – may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'[146]

Since the passage of *Jones*, lower courts have similarly expressed concerns that a decrease in the cost of conducting surveillance may undermine traditionally available practical privacy protections. In *Tracey v. State*, the Florida Supreme Court held that real time cell site location data was protected by the Fourth Amendment.[147] In so doing, the court particularly noted that long-standing concerns about the government's ability to obtain information about individuals without consulting a magistrate seem "prescient now that technology has advanced to the point that our whereabouts can be ascertained easily and at low cost by the government."[148] The Florida Supreme Court further grounded their concerns about law enforcement access to inexpensive methods of collecting data in the historical policy goals of the Fourth Amendment, stating that "the ease with which the government, armed with current and ever-expanding technology, can now monitor and tack our cell phones, and thus ourselves, with minimal

---

[141] *United States v. Jones*, *supra* note 84, at 963-4. The Supreme Court estimated that, without the use of an electronic device, the surveillance at issue in this case "would have required a large team of agents, multiple vehicles, and perhaps aerial assistance." *Id.*

[142] *Id.*

[143] *Id.* at 964.

[144] *Id.* at 964.

[145] "I join the Court's opinion because I agree that a search within the meaning of the Fourth Amendment occurs, at a minimum, '[w]here, as here the Government obtains information by physically intruding on a constitutionally protected area.'" *Id.* at 954.

[146] *Id.* at 956.

[147] *Tracey v. State*, 152 So.3d 504 (2014).

[148] *Id.* at 512.

expenditure of funds and manpower, is just the type of 'gradual and silent encroachment' into the very details of our lives that we as a society must be vigilant to prevent."[149]

Even as courts recognize the role that declining practical limitations play in facilitating law enforcement use of surveillance, they have been reticent to establish a clear standard for determining when law enforcement use of inexpensive surveillance constitutes a search. Justice Alito's concurring opinion in *Jones* contended that the continuous, long-term use of a GPS tracker constituted a Fourth Amendment search while explicitly avoiding setting forth a threshold for determining when a search had occurred. Rather, there was no need to "identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark."[150] Similarly, in *Tracey v. State*, the Florida Supreme Court refused to adopt a framework for determining whether real time cell site monitoring is of a sufficient duration to constitute a violation of the Fourth Amendment.[151] Instead, they characterized cell phones as an essential part of modern life,[152] and found that the defendant's real time cell phone location information was protected under the reasonable expectation of privacy test.[153]

3. Scholarly Reactions

The role of declining practical protections for privacy has been the subject of significant academic interest. Given the ambiguity of judicial opinions recognizing the role of practical limitations in protecting individuals who are targeted by police, it is unsurprising that several academics have turned to more concrete methods of determining when technology has reduced privacy protections to the point that additional legal protections may be warranted. Many of these methods require quantitatively or empirically comparing the effects of technological advances to some pre-technology benchmark, which may prove problematic.

As initially imagined, equilibrium-adjustment theory does not require using empirical or quantitative standards to determine whether a new form of technology has reduced practical protections to the point that additional legal protections may be required. According to Kerr one of the strengths of equilibrium-adjustment theory is that it allows judges to make decisions

---

[149] *Id.* at 522. The Florida Supreme Court is echoing a quote attributed to James Madison, who "is reported to have observed, 'Since the general civilization of mankind, I believe there are more instances of the abridgement of freedom of the people by gradual and silent encroachments by those in power than by violent and sudden usurpations.'" *Id.*

[150] *Id.* at 964.

[151] *Tracey v. State*, 152 So.3d at 521 ("Nor can we avoid this danger by setting forth a chart designating how many hours or days of monitoring may be conducted without crossing the threshold of the Fourth Amendment.").

[152] *Id.* at 523.

[153] *Id.* at 525.

without empirical data.[154] Indeed, "[a] dramatic mismatch exists between the difficulty and complexity of the problem of regulating police investigations and the empirical evidence judges have about what rules work or what the impact of a possible new rule might be."[155] Equilibrium-adjustment theory is intended to be used intuitively, to allow judges to make decisions about the impact of new technology by using "the lessons of shared experience with past rules to help judges identify the likely impact of new Fourth Amendment rules."[156]

Several scholars have expanded upon equilibrium-adjustment theory in order to describe how it could be implemented in practice. Several of these efforts recommend establishing quantitative or empirical standards for determining whether technology has evolved to the point that additional legal protections may be warranted. For example, Paul Ohm identifies several difficulties with applying an equilibrium-adjustment approach in practice,[157] and then suggests that the approach should instead focus on how technology has changed outcomes related to criminal investigations.[158] Under this approach, "[t]he ultimate question should be: How has technology altered the *metrics* of crime fighting? Are more people going to prison? Fewer? Are leads easier to develop today? Harder? How long does each investigative step take to accomplish?"[159] Ohm eventually narrows these questions down to one "admittedly unorthodox proposal: it should take, on average, just as long to solve a crime today as it has in the past."[160]

Similarly, Bankston and Soltani suggested a further refinement of the equilibrium-adjustment approach by suggesting that the analysis focus on changes in the cost to law enforcement of conducting surveillance.[161] Specifically, they propose "a rough rule of thumb: If the cost of the surveillance using the new technique is an order of magnitude (ten times) less than the cost of the surveillance without using the new technique, then the new technique violates a reasonable expectation of privacy."[162] They support this proposition by analyzing the cost of tracking a suspect's location using various methods, and demonstrating that traditional, in-person surveillance can be 53 times as expensive as tracking a person using their cell phone.[163]

---

[154] Kerr, *supra* note 101, at 535.

[155] *Id.*

[156] *Id.* at 535-6.

[157] Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 Miss. L. J. 1309, 1343 (2012). These difficulties include the need to determine whether an emerging technology provides more assistance to law enforcement or criminals, changes in technology, limited judicial understanding of emerging technologies, difficulties in framing the problem, and need to develop stopping criteria for this analysis. *Id.* at 1341-1345.

[158] *Id*. at 1346.

[159] *Id.*

[160] *Id.*

[161] Bankston and Soltani, *supra* note 53.

[162] *Id*. at 351.

[163] *Id*. at 354.

However, there are significant difficulties in implementing such empirical or quantitative approaches for determining whether technology has eroded practical limitations on law enforcement surveillance to the point that additional legal protections might be required. For instance, these approaches largely suffer from status quo bias, despite the fact that the current balance of power between the individual and the state may not be ideal from either societal or constitutional perspectives. Additionally, different types of law enforcement agencies vary in significant ways that may affect their ability to adapt to changes in technology.

II. Variation in Law Enforcement Agencies

When analyzing the role of practical limitations in protecting privacy against invasive government searches, most scholars focus on the variety of technologies that facilitate cheaper and easier searches.[164] Very little attention is paid to heterogeneity on the other side of the equation: variation in the law enforcement agencies who seek to use surveillance. This is particularly problematic, as "it is abundantly evident that small-town police departments stand in stark contrast to the dominant big-city model."[165] Different types of law enforcement agencies face different resource constraints and engage in different decision making processes, and consequently may be affected differently by changes in the cost and difficulty of using electronic surveillance. If the Fourth Amendment is to be interpreted in order to "restore the status quo ante level of government power"[166], then variation in ability of different law enforcement agencies to conduct searches creates difficulty in both establishing and restoring this status quo.

This section discusses in the available resources and manpower across different types of law enforcement agencies that operate in the United States. For purposes of this analysis, Federal and state agencies are ignored, to focus only on variation in the local law enforcement agencies that employ approximately 80% of law enforcement officers in the United States.[167] Variation

---

[164] *See, e.g.*, Renee McDonald Hutchins, *Tied Up in Knotts? GPS Technology and the Fourth Amendment*, 55 UCLA L. Rev. 409 (2007); Ric Simmons, *From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 Hastings L. J. 1303 (2002); Surya Gablin Gunasekara, *The March of Science: Fourth Amendment Implications on Remote Sensing in Criminal Law*, 36 J. Space L. 115 (2010).

[165] David N. Falcone, L. Edward Wells, and Ralph A. Weisheit, The small-town police department, 25 Policing Int'l J. Police Strat. & Mgmt. 371, 381 (2002).

[166] *Kerr*, *supra* note 101, at 480.

[167] According to the 2014 edition of *Crime in the United States*, there are 627,949 city and county law enforcement officers (excluding civilian employees) and 38,890 state and tribal law enforcement officers (excluding civilian employees). Federal Bureau of Investigation, *2014 Crime in the United States* (2014). According to the latest data from the Bureau of Justice Statistics, in 2008 there were approximately 120,000 federal officers "authorized to make arrests and carry firearms." Brian A. Reaves, *Federal Law Enforcement Officers, 2008*, Bureau of

between agencies that police small communities and agencies that police large communities is explored, and this section concludes by briefly summarizing and discussing my findings.

Wherever possible, variation across different types of law enforcement agencies is quantitatively described, based on publicly available data from two sources. First, data on law enforcement resources, personnel, and activities is used from the 2013 edition of the Law Enforcement Management and Administrative Statistics (LEMAS) survey published by the Bureau of Justice Statistics.[168] These data are obtained through a survey periodically administered to a nationally representative sample of 3,000 law enforcement agencies.[169] Second, data on criminal activity known to law enforcement is used from the 2013 edition of the Uniform Crime Reporting (UCR) Program data.[170]

Because both datasets contain a unique identifier for every law enforcement agency reporting data, it is possible to associate the law enforcement resource information from LEMAS with the criminal activity information from the UCR. To understand variation in the resources available to local law enforcement agencies, state, county, and tribal law enforcement agencies were omitted, as well as any agency that did not report data in both LEMAS and the UCR. This left me with 2,659 agencies in the sample. These remaining were divided into four groups, based on the size of the population served by the agency. The number of agencies in each group is reported in table 4.1 below.

Table 4.1. Number of Law Enforcement Agencies Included in Sample

Size of Population Served	N
Fewer than 50,000 people	1727
Between 50,000-200,000 people	658
Between 200,000-1,000,000 people	238
More than 1,000,000 people	36
Any	2659

Justice Statistics Bulletin NCJ 238250 (June 2012), *available at http://www.bjs.gov/content/pub/pdf/fleo08.pdf*.

[168] These data can be conveniently accessed through the National Archive of Criminal Justice Data at the Interuniversity Consortium for Political and Social Research. *See* Bureau of Justice Statistics, *Law Enforcement Management and Administrative Statistics (LEMAS), 2013*, http://www.icpsr.umich.edu/icpsrweb/NACJD/studies/36164.

[169] Bureau of Justice Statistics, *Data Collection: Law Enforcement Management and Administrative Statistics (LEMAS)*, http://www.bjs.gov/index.cfm?ty=dcdetail&iid=248.

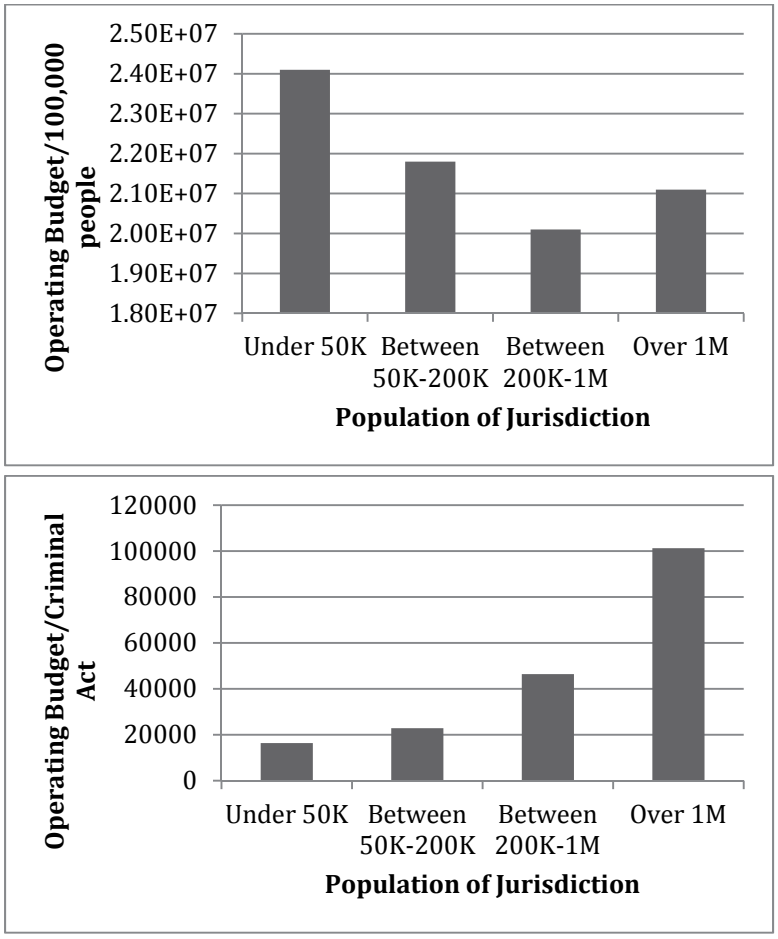
[170] Federal Bureau of Investigations, *Uniform Crime Reporting Program Data: Offenses Known and Clearances by Arrest, 2013*, https://www.icpsr.umich.edu/icpsrweb/ICPSR/studies/36122.

A. Variation in Resources

1. Variation in Funding

Because of the increasing attention paid to the role of cost in regulating law enforcement use of electronic surveillance, this section begins by describing variation in the operating budget across agencies serving different size communities. Figure 4.1 below describes the average operating budget[171] of law enforcement agencies in each group in two different ways. First, the operating budget is calculated per 100,000 people residing in the community; next, the operating budget is calculated per criminal act investigated.

Figure 4.1. Variation in Resources Available to Law Enforcement



[171] As defined by LEMAS, an agency's operating budget does not include "construction costs, major equipment expenditures, or other capital expenditures." *Bureau of Justice Statistics, Law Enforcement Management and Administrative Statistics (LEMAS), 2013: Codebook*, 164 (2013).

As can be seen, law enforcement agencies in small communities spend much more per resident than law enforcement agencies in large communities, but much less per criminal act. This apparent discrepancy might be explained in several ways. First, larger law enforcement agencies typically investigate more crimes, and may be able to take advantage of economies of scale to conduct these investigations more efficiently. Second, small and large agencies may face different types of crimes. If more sophisticated criminal acts take place in larger communities, law enforcement may require additional resources to investigate them. Third, larger agencies may have a broader tax base or be better situated to seek state and federal grants, and therefore may have more resources available to devote to investigating crimes.

2. Variation in Funding Sources and Partnerships

Law enforcement agencies may receive funds from a variety of sources. While external sources of funding may allow agencies to undertake activities that could not otherwise be supported by their tax base, the source of the funding may dictate who can receive the money and how the money may be used. For example, the Department of Homeland Security funds "high-threat, high-density urban areas" through their Urban Area Security Initiative (UASI).[172] The Department of Homeland Security funds smaller localities through their state governments; the State Homeland Security Program (SHSP) provides money to states which then may be passed to local jurisdictions.[173] In either case, a quarter of the funds provided through each grant must be dedicated to terrorism prevention.[174] Similarly, the Bureau of Justice Assistance administers the Edward Byrne Memorial Justice Assistance Grant Program, which allocates funding to a wide variety of state and local agencies.[175] Funds granted under this program cannot be used to purchase certain types of heavy munitions,[176] and approval must be granted before certain types of other expenditures can be made.[177]

Figure 4.2 below shows the percentage of law enforcement agencies that receive operational funding from county, state, and federal sources, differentiating by the size of the jurisdiction served by the agency.

---

[172] Department of Homeland Security, *DHS Announces Funding Opportunity for Fiscal Year (FY) 2016 Preparedness Grants*, Feb. 16, 2016, https://www.dhs.gov/news/2016/02/16/dhs-announces-funding-opportunity-fiscal-year-fy-2016-preparedness-grants.

[173] *Id.*

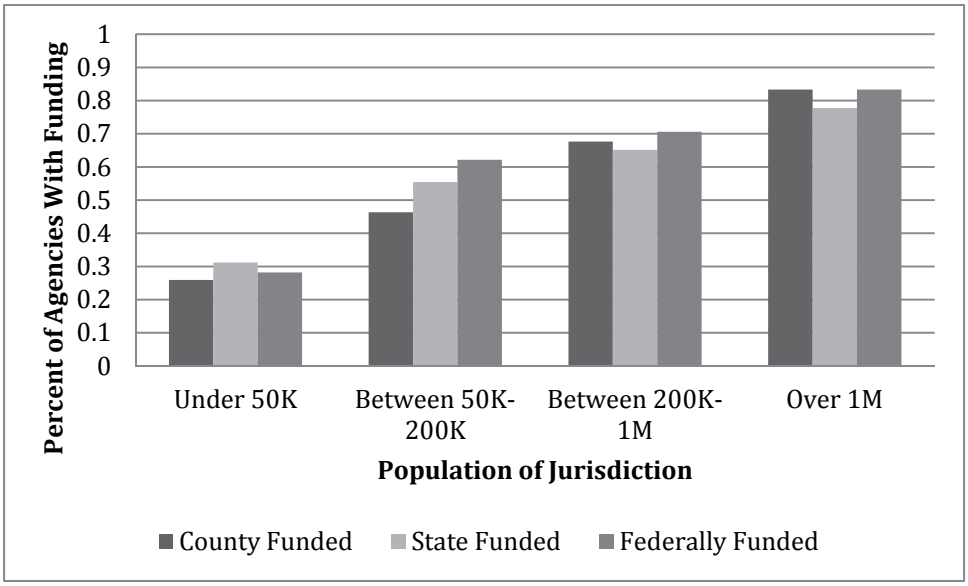
[174] *Id.*

[175] Bureau of Justice Assistance, *Edward Byrne Memorial Justice Assistance Grant (JAG) Program*, https://www.bja.gov/ProgramDetails.aspx?Program_ID=59.

[176] These heavy munitions include "[f]irearms and/or ammunition with a caliber of .50 or higher," "[g]renade [l]aunchers," and "[b]ayonets." Bureau of Justice Assistances, *Edward Byrne Memorial Justice Assistance Grant (JAG): Prohibited and Controlled Expenditures*, https://www.bja.gov/Funding/JAGControlledPurchaseList.pdf.

[177] *Id.* Controlled but not prohibited expenditures include armored vehicles, boats, real estate, construction projects, and explosives.

Figure 4.2. Variation in Sources of Funding



Data from LEMAS shows that larger law enforcement agencies may receive more external funding. 83.3% of agencies that serve communities with more than 1,000,000 people reported receiving federal funds; 28.1% of agencies that serve communities with fewer than 50,000 people reported receipt of federal funds. This may be due in part to the existence of specialized funding programs designed for larger cities. Additionally, even if local law enforcement agencies are eligible for funding from state and federal agencies, onerous requirements and procedures for receiving this money may pose a barrier to the use of funds by small localities.[178]

However, LEMAS only provides data on sources of funding used for operational expenses, and does not include funding used for major equipment outlays. Local law enforcement departments may receive other resources from state and federal agencies specifically for procuring equipment. Some federal agencies, including the Department of Justice, Department of Defense, and Department of Homeland Security, can directly transfer equipment to local law enforcement.[179] This equipment often consists "routine" supplies such as "office furniture, computers and other technological equipment, personal protective equipment and basic

[178] For example, "[m]ost states have a 100 percent reimbursement system, under which no funds are advanced to localities before the purchases are actually made. This can be a real problem for towns with small budgets." Wise and Nader, Developing a National Homeland Security System in Intergovernmental Management for the 21st Century, pg. 90.

[179] Executive Office of the President, *Review: Federal Support for Local Law Enforcement Equipment Acquisition*, https://www.whitehouse.gov/sites/default/files/docs/federal_support_for_local_law_enforcement_equipment_acquisition.pdf.

firearms", but may also involve "military equipment, including high powered weapons and tactical vehicles."[180]

While there are no global statistics showing which agencies receive equipment through these all of programs, it does appear that both small and large agencies receive support. For example, the 1033 program, through which the Department of Defense shares equipment with state and local law enforcement, has provided over $5 billion worth of equipment to thousands of law enforcement agencies across the United States,[181] including agencies in large urban counties such as Los Angeles County (California) and small rural counties such as Bibb County (Alabama).[182] According to a database of transfers compiled by the Pentagon and released by the New York Times,[183] most of the equipment transferred consists of weaponry, tools, and outdoors and protective gear.[184] There are few entries that could conceivably be related to electronic surveillance, such as computer equipment and video recording/receiving devices.[185]

3. Variation in Access to Surveillance Devices

Agencies in that respond to LEMAS are asked to describe whether they employed certain information gathering techniques, including several types of electronic sources of information. Figure 4.4 below describes the percent of agencies in each category that reported using three forms of electronic information gathering: license plate readers, smartphones, and surveillance cameras.

---

[180] *Id.* at 3.

[181] Shawn Musgrave, Tom Meagher, and Gabriel Dance, *The Pentagon Finally Details its Weapons-for-Cops Giveaway*, The Marshall Project, https://www.themarshallproject.org/2014/12/03/the-pentagon-finally-details-its-weapons-for-cops-giveaway#.UNpKD9GbA (2014).

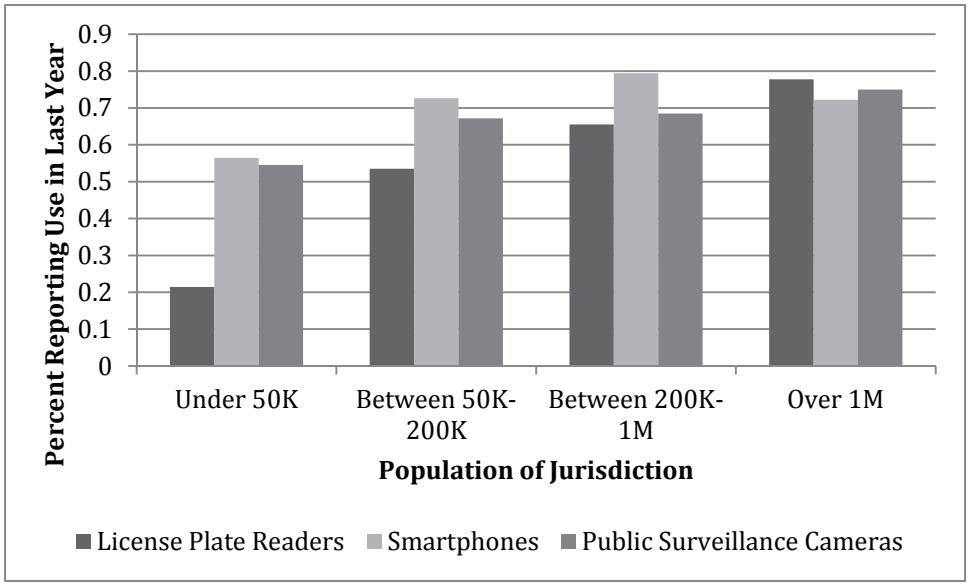
[182] Matt Apuzzo, *What Military Gear Your Local Police Bought*, The New York Times, http://www.nytimes.com/2014/08/20/upshot/data-on-transfer-of-military-gear-to-police-departments.html?_r=1 (2014).

[183] The New York Times has since published this database on Github. *Available at* https://github.com/TheUpshot/Military-Surplus-Gear.

[184] *Id.*

[185] *Id.*

Figure 4.4. Variation in Types of Surveillance Tools Used



As can be seen, the most significant difference between different categories of agency occurs for license plate readers. Roughly 20% of agencies serving the smallest populations use license plate readers, while almost 80% of agencies serving the largest populations use these readers. This variation may be due to the cost of obtaining equipment, differences in capacity to engage with newer forms of surveillance, or differences in the surveillance needs of the different types of organizations.

B. Variation in Manpower

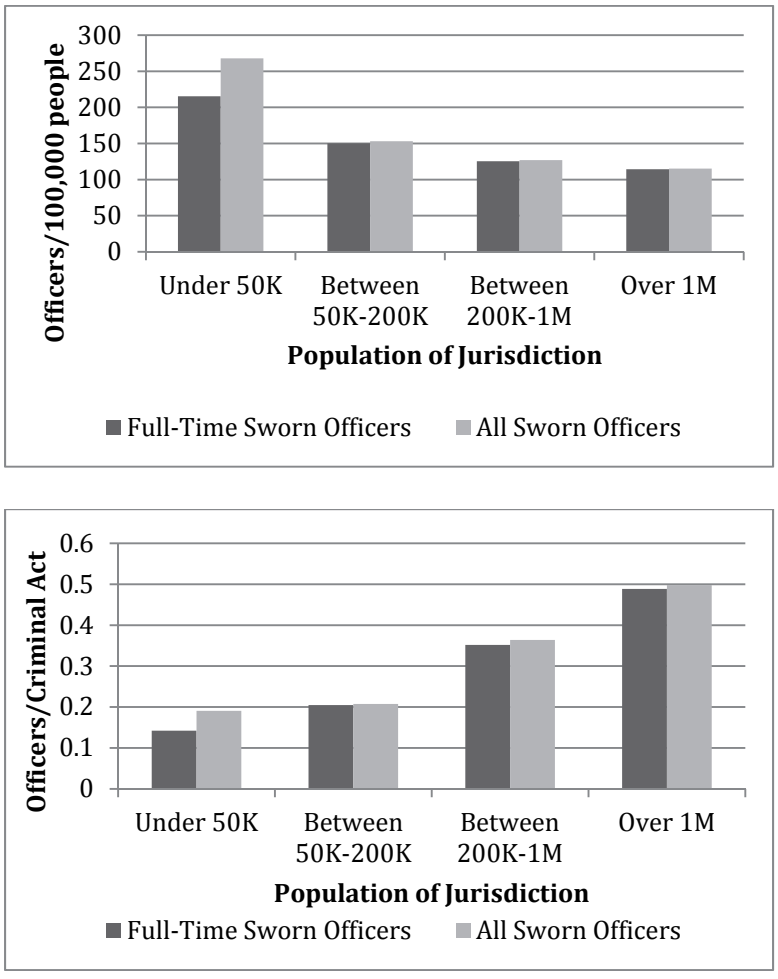
1. Variation in Size of Police Force

Even though technological surveillance has been described as a force multiplier,[186] manpower availability still plays a crucial role in determining whether or not a law enforcement

[186] "With tightening budgets, and recruitment and retention always a struggle, law enforcement departments need to look to technology to swell its ranks. Los Angeles (California) Police Department (LAPD) Chief William Bratton has long spoken of technology as a 'force multiplier.'" Paul Davis, *Technology serves as a force multiplier*, Officer.com, http://www.officer.com/article/10249729/technology-serves-as-a-force-multiplier (2007). However, the use of technology as a force multiplier may be difficult to quantify, and may be impossible to realize in all circumstances. *See* Tom Barry, *Fallacies of High-Tech Fixes for Border Security*, Center for International Policy, https://www.ciponline.org/research/html/fallacies-high-tech-fixes-border-security (2010) ("But the DHS report of December 2005 found that the Border Patrol was 'unable to quantify force-multiplication benefits' and noted among the many flaws of ISIS was that the project was badly undermanned, especially in monitoring the output of the surveillance system.").

agency can conduct surveillance. While the amount of participation needed from officers varies across different types of electronic surveillance, law enforcement officers are still needed to conduct the surveillance and interpret the results. Figure 4.5 below describes the variation in law enforcement officers across jurisdictions that serve communities of various size. The available manpower is described in two ways: first, in terms of the population of the community; second, in terms of the number of criminal activities investigated by law enforcement.

Figure 4.5. Variation in Law Enforcement Manpower



As can be seen, the available manpower varies across different types of jurisdictions in much the same way that operating expenses vary. While smaller jurisdictions have a higher proportion of law enforcement officers per capita than larger agencies, they have a smaller number of officers per criminal act known to law enforcement. The relationship between manpower and operating budget is unsurprising, given that the operating budget is used to pay the salaries of sworn officers.

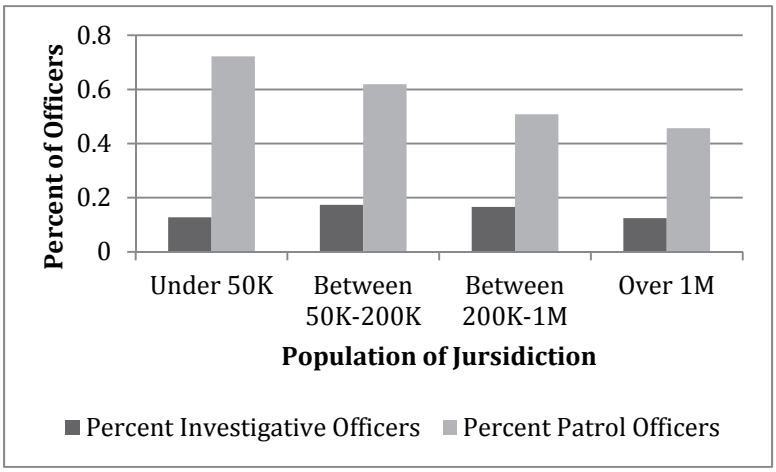
For all agencies, both the number of full-time sworn officers and all sworn officers (including part-time officers) is presented. Only agencies serving the smallest population category show a significant percentage of part-time sworn officers. The employment of part-time sworn officers may allow very small communities to maintain a sufficiently robust police force in a cost efficient manner.[187]

2. Variation in Activities Undertaken by Officers

Law enforcement officers are not fungible: different officers have different capabilities and engage in different activities. This is particularly important in the case of electronic surveillance. Since officers with certain skills may be necessary to employ some forms of electronic surveillance, agencies that employ few of these officers may be less able to conduct electronic surveillance. As law enforcement officers develop much of their expertise through on-the-job training, officers who regularly use electronic surveillance could be expected to be most knowledgeable about how it should be used. Consequently, agencies that engage in the types of activities that are more likely to involve electronic surveillance may be more likely to have officers skilled in the use of electronic surveillance.

Figure 4.6 below describes the percentage of law enforcement officers engaged in investigatory or patrol roles for each category of law enforcement agency.

Figure 4.6 Variation in Types of Law Enforcement Officers[188]



[187] It should also be noted that a particular jurisdiction may be policed by more than one agency; for example, a particular town may be policed both by their own police force and the county sheriff's office. Overlapping jurisdiction may be another way of ensuring cost effective policing.

[188] These categories do not sum to 100% because law enforcement officers may be primarily engaged in other activities, such as protecting courthouses.

As can be seen, the percentage of investigative officers is roughly stable across jurisdictions serving all sizes of community. However, agencies serving small communities employ a larger percentage of patrol officers then agencies serving large communities. This may be due in part to the other roles taken on by law enforcement officers in larger communities. For example, small communities may be less likely to run their own jails or protect their own courthouses, while law enforcement officers in larger communities may serve in these capacities.

Some law enforcement agencies have specialized units within their department that either investigate particular types of crimes or engage with certain types of investigative techniques. Officers in specialized departments that frequently use electronic surveillance may have a greater opportunity to develop expertise in electronic surveillance use, and can additionally serve as a resource for other officers who need to use electronic surveillance occasionally. For example, the New York Police Department has a specialized unit that deals with gathering information from social networking sites.[189] "The NYPD's approach is that special social media units can provide information to patrol officers or others who need it, and that patrol officers should remain focused on their duties on the street, rather than studying social media on their own."[190] Officers in other specialized units that frequently search social media sites receive their own on-the-job training, focused on how social media is used by their unit.[191]

LEMAS requests information about specialized task forces used by each responding department. This analysis focuses on those task forces that are more likely to involve electronic surveillance: namely, those related to cybercrime, terrorism, gangs, or special operations. For purposes of this analysis, an agency is defined as having a task force if they had any personnel dedicated to an issue. Figure 4.7 below describes variation in the existence of task forces across different types of agencies.

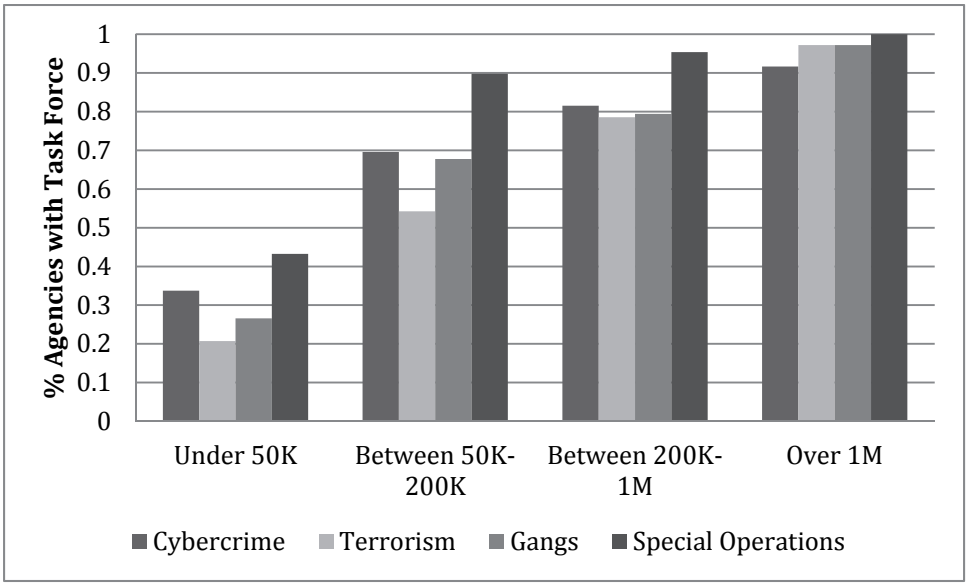
---

[189] *Social Media and Tactical Considerations for Law Enforcement*, Department of Justice Community Oriented Policing Services and Police Executive Research Forum, at 16, http://www.policeforum.org/assets/docs/Free_Online_Documents/Technology/social%20media%20and%20tactical%20considerations%20for%20law%20enforcement%202013.pdf (2013).

[190] *Id*. at 16.

[191] *Id.*

Figure 4.7. Variation in Specialized Task Forces



As can be seen, there is a sharp difference between specialized task force use in law enforcement departments in small communities versus law enforcement departments in large communities. For example, just 20.7% of the departments in small communities had at least some personnel dedicated to terrorism, while over 97% of the departments in large communities had at least some personnel dedicated to terrorism. As the large departments surveyed more frequently report having personnel dedicated to activities that often involve electronic surveillance, these data suggest that large departments may have more in-house expertise in engaging in electronic surveillance.

3. Variation in Officer Characteristics

In this section, variation in officer characteristics across jurisdictions that serve different types of jurisdictions is discussed, focusing on those characteristics that have been shown to affect either law enforcement decision making or technology uptake.

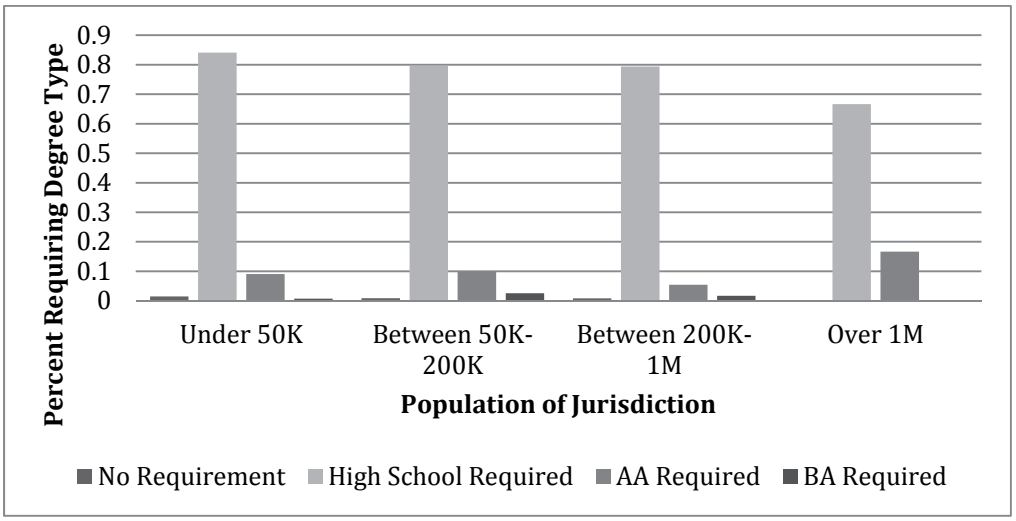
Researchers have extensively studied how educational attainment affects law enforcement behavior and decision-making. Although the research is somewhat mixed, law enforcement officers with college educations appear to use force less often,[192] be more innovative,[193] and rate

[192] Jason Rydberg and William Terrill, *The Effect of Higher Education on Police Behavior*, 13 Police Quarterly 92 (2010).

[193] Roy Roberg and Scott Bonn, *Higher education and policing: where are we now?*, 27 Policing 469, 475 (2004).

their ability to accept changes more highly.[194] While the effects of educational attainment on law enforcement use of electronic surveillance has not been studied, increased educational attainment has long been associated with increased uptake of new technologies generally,[195] and uptake of technology in the workplace specifically.[196] Although LEMAS does not include data on the actual educational attainment of law enforcement officers, it does describe the minimum educational requirements of each agency included in the survey, shown in Figure 4.8 below.

Figure 4.8. Variation in Minimum Education Requirements



As can be seen, while most departments of any type require a high school degree for employment, law enforcement departments that serve large communities may require more educational attainment than law enforcement departments that serve small communities. 84.13% of law enforcement agencies in communities with fewer than 50,000 people require new law enforcement officers to have only a high-school degree; 66.67% of law enforcement agencies in communities of more than one million people hired individuals with only a high school diploma.

Demographic differences have also been shown to be associated with difference in technology uptake, including technology uptake in the workforce. Some researchers have argued

---

[194] Suman Kakar, *Self-evaluations of police performance: An analysis of the relationship between police officers' education level and job performance*, 21 Policing 632, 639 (1998).

[195] "As noted, a common finding in the adoption literature is that more educated agents are more likely to adopt new technologies." Andrew D. Foster and Mark R. Rosenzweig, *Microeconomics of Technology Adoption*, 2010 Annu. Rev. Econom. 1, 17 (2010). *See also* Gregory D. Wozniak, *Human Capital, Information, and the Early Adoption of New Technology*, 22 J. Human Resources 101 (1987).

[196] Adam Baumgart-Getz, Linda Stalker Prokopy, and Kristin Floress, *Why farmers adopt best management practice in the United States: A meta-analysis of the adoption literature*, 96 J. Environ. Manage. 17 (2012).

that gender affects how users interact with new technology in the workplace. According to Venkatesh and Morris (2000), "men's technology usage decisions were more strongly influenced by their perceptions of usefulness," while "women were more strongly influenced by perceptions of ease of use and subjective norm."[197] Age also appears to play a role in determining whether and how new workplace technology is adopted. For example, Morris and Venkatesh (2000) found that "younger workers' technology usage decisions were more strongly influenced by attitude toward using the technology" while "older workers were more strongly influenced by subjective norm and perceived behavioral control."[198]

While LEMAS does not collect or report information on the age of officers employed by responding agencies, it does provide data on the proportion of men and women employed by each agency. These data show that agencies in small jurisdictions employ a higher percentage of men then agencies in large jurisdictions, although the difference is slight. On average, 92.1% of officers at agencies serving communities of under 50,000 people are male; 85.3% of officers at agencies serving communities of over 1 million people are male.

C. Summary and Discussion

The above analysis reveals several key differences between law enforcement agencies that serve small communities and law enforcement agencies that serve large communities. All-in-all, departments in large communities have several advantages that may make it easier for them to utilize electronic surveillance. Most significantly, law enforcement agencies in large cities are capable of devoting personnel to types of investigations that frequently require electronic surveillance, thus allowing these personnel to develop expertise in electronic surveillance. Officers in large departments tend to be better educated, which may make them more able to adapt to changes in technology. Finally, the law enforcement departments in large communities more frequently reported receiving external funding for operating expenses, suggesting that they may be able to undertake activities that could not be supported solely through their tax base.

Law enforcement departments from small communities did report advantages that may improve their ability to undertake electronic surveillance. Smaller communities reported having more resources available per person in their jurisdiction, in terms of both available funds and available manpower. However, this advantage disappears if resources are considered as a function of crimes reported rather than people living in the jurisdiction. Furthermore, if smaller jurisdictions are policed by more than one agency, it may be possible for them to mitigate their

---

[197] Viswanath Venkatesh and Michael G. Morris, *Why Don't Men Ever Stop to Ask for Directions? Gender, Social Influence, and Their Role in Technology Acceptance and Usage Behavior*, 24 MIS Quarterly 115, 115 (2000).

[198] Michael G. Morris and Viswanath Venkatesh, *Age Differences in Technology Adoption Decisions: Implications for a Changing Work Force*, 53 Personnel Psychology 375, 375 (2000).

inexperience with using electronic surveillance by learning from other, more experienced agencies.

To consider how the differences between large and small departments might impact their ability to take advantage of decreasing practical limitations, consider a hypothetical small-town police department and a hypothetical large city police department, with characteristics that roughly correspond to the averages obtained through the LEMAS data. Table 4.2 below describes how these departments would be affected by particular technological developments that might reduce practical limitations on law enforcement surveillance.

Table 4.2. Impact of Variation on Practical Limitations

	Large Law Enforcement Agencies	Small Large Enforcement Agencies
Low Marginal Costs; Low Fixed Costs	Able to pay low marginal and low fixed costs; able to use surveillance with few financial barriers	Fewer resources per crime suggest may be less able to afford surveillance unless costs are very low; but still able to use electronic surveillance more often as costs are reduced
Low Marginal Costs; High Fixed Costs	Able to pay high fixed costs, and therefore be able to use surveillance with low financial barriers	May be unable to pay high fixed costs, and therefore be entirely unable to use surveillance
Commercial Collection of Data	Frequent users of commercial data; more experience creates more expertise in locating and requesting commercial data; may have specialized units that request this information	Less frequent users of commercial data; lack of repetition makes it more difficult to develop and apply expertise in using commercial data

As new forms of electronic surveillance are developed which allow law enforcement to obtain information with low marginal costs and low fixed costs, the large city police department would appear to be better able to take advantage of the reduced costs than the small-town police department, although this difference may be minimal. Assuming that the cost of using the surveillance is the same across both departments, the large urban police department has a greater operating budget per reported crime, and could therefore afford to adopt new forms of surveillance more quickly as the price decreases. Furthermore, as large urban police departments have more specialized personnel, they may be more aware of new low cost surveillance options and therefore able to adopt these options more quickly. The small town police department may have more difficulty adjusting. It is possible that new forms of surveillance might have lower cost, but still be too expensive for a small town police department to utilize on a regular basis, given their available operating budget per crime. Additionally, the small town police department may have fewer opportunities to discover lower cost forms of surveillance, and they are less likely to have specialized personnel who would be likely to seek out new forms of surveillance.

The development of new forms of electronic surveillance with low marginal costs but high fixed costs would have even more of a differentiating effect between the big city and small town

police departments. The big city police department would be better able to pay the initial fixed cost, since they have a greater overall budget. They would also probably receive a greater return on their investment: since they serve a larger jurisdiction, once they had paid the initial fixed cost, they would have more opportunities to utilize the particular form of surveillance.[199] On the other hand, the smaller department would both be less able to pay the initial fixed cost, and would reap fewer benefits from doing so. Consequently, the small town police department would be less likely to adopt a form of surveillance with high fixed costs and low variable costs.

Finally, the big city police department would be better positioned to take advantage of increases in commercial collection of data. In order to take advantage of commercially collected data, law enforcement agencies must be aware that a commercial entity may have collected data that is relevant to a criminal investigation and be able to successfully request this data from the commercial entity.[200] Because of the constantly changing technological and commercial landscape, these steps are non-trivial. The big city police department and the small town police department would not be equally able to take these steps. The big city police department would be more likely to have specialized units or officers with extensive training in obtaining information from commercial entities. Additionally, even if the big city police department does not have such a specialized unit, as they investigate more crimes, they are likely to request commercial information more often and therefore be more aware of developments in technology.

In sum, it appears that practical limitations on law enforcement surveillance may fall faster in big cities. Law enforcement departments that serve larger jurisdictions can develop specialized surveillance skills, which may better position them to take advantages of innovations in technology and decreasing surveillance costs. The apparent variation in practical protections against law enforcement use of surveillance raises an important question: if the Fourth Amendment should be interpreted in light of technological changes that affect the practical protections available to individuals targeted by law enforcement, should this interpretation also take into account how these practical protections vary across different jurisdictions?

---

[199] Indeed, the big city police department might not only have more opportunities to use the new form of surveillance, but might also be incentivized to use it more often in order to justify the cost of purchasing the equipment. Analogous behaviors have been observed in health care providers, who must utilize expensive equipment at a rate that justifies the cost. For example, the American College of Physicians noted that "[t]o cover the cost of leasing an MRI machine, an office needs to perform approximately four scans per day per scanner….The excess capacity and high prices in the U.S. translates into some $40 billion of additional cost to the U.S. health care system." American College of Physicians, *Controlling Health Care Costs While Promoting the Best Possible Health Outcomes*,10 (2009) *available at* https://www.acponline.org/acp_policy/policies/controlling_healthcare_costs_2009.pdf.

[200] *See* discussion *supra* II.B.

III. Addressing the Impact of Variation on Practical Limitations

This section argues that it is critical to consider variation in law enforcement's ability to take advantage of changes in technology when determining how the Fourth Amendment should be interpreted in light of technological changes. Refusing to acknowledge the difficulties smaller law enforcement agencies face when adopting new technologies creates further difficulties for these smaller agencies. As new technologies are developed that make it easier for law enforcement to gather information, interpreting the Fourth Amendment to restore the balance of power between the individual and the state in large cities may in fact undermine this balance in smaller jurisdictions. In other words, a Fourth Amendment jurisprudence that is crafted based on how surveillance is used in large urban jurisdictions may prove detrimental in smaller jurisdictions.

The existence of variation among law enforcement agencies does not necessarily imply that this variation should be considered when interpreting the Fourth Amendment in light of emerging technology and disappearing practical protections for individuals targeted by law enforcement surveillance. One might argue that it is only necessary to focus on surveillance use in large cities: if smaller jurisdictions are unable to adopt a new technology, then this new technology will simply not impact either law enforcement or individual rights in that community. It may be that courts can reestablish the balance between police power and individual privacy dictated by the Fourth Amendment by analyzing only the effects of emerging technology on big city police agencies, with minimal deleterious effects on the balance between police power and individual privacy in smaller communities.

However, there are several reasons to believe that crafting Fourth Amendment jurisprudence based on how technology has shifted the balance of power between police power and individual privacy in urban environments only may further upset this balance in smaller communities. First, innovations that make it easier for law enforcement to collect information during criminal investigations do not occur in a vacuum. Technological advances are changing not just how law enforcement operates, but also how both criminals and the general public conduct the activities of daily life. Simply because law enforcement officers in smaller jurisdictions are less able to adapt new investigative technologies does not mean that criminals operating in smaller jurisdictions are less able to adopt new technologies that make it easier to conceal their illegal behavior. For example, it has been suggested that criminals may be more likely to adopt electronic communications, since it is less likely that law enforcement will observe illegal electronic communications than illegal in-person communications.[201]

[201] "The use of third parties has a substitution effect. It in enables wrongdoers to take public aspects of their crimes and replace them with private transactions." Orin Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561, 573 (2009).

Making it more difficult for law enforcement departments in smaller jurisdictions to adopt emerging technologies may exacerbate the effects of current technological trends that make it more difficult for law enforcement to conduct long-used forms of electronic surveillance. Law enforcement agencies and advocates have argued that the increased availability of easy-to-use encryption technology has made sources of communications information "go dark": in other words, "law enforcement personnel have the 'legal authority to intercept and access communications and information pursuant to court order,' but 'lack the technical ability to do so.'"[202] Some scholars have argued that the availability of new, emerging sources of information may help compensate for those sources of information that are going dark.[203]

Although the idea that new sources of information may make up for the loss of traditional sources of information has a great deal of intuitive appeal, the significant variation across different types of law enforcement departments suggests that this may not be the case for all localities. Rather, large departments will be able to take advantage of new sources of information, while small departments lack the resources and the repeat exposure to new sources of information necessary to develop expertise.[204] While large departments may indeed be able to enter a golden age of surveillance, smaller departments will be left in the dark.

Second, imposing legal restrictions on law enforcement surveillance in smaller communities before these agencies have developed the capability and capacity to engage in certain types of surveillance may make these developments more difficult later on. Law enforcement officers receive much of their training on-the-job, generally from more experienced officers in their department. If the veteran officers in a particular small town police department do not adopt electronic surveillance, then the officers they train will be less likely to view electronic surveillance as part of their crime-solving toolbox and will consequently be less likely to utilize it during criminal investigations. This disadvantage does not end once the training period is complete. Officers are likely to ask their colleagues for suggestions during an investigation; those colleagues cannot suggest electronic surveillance as an opinion if they are unfamiliar with it. In other words, the choices an officer makes during an investigation are influenced by the culture of their department. If it is too difficult for a particular department to utilize electronic

---

[202] House Homeland Security Committee Majority Staff Report, *Going Dark, Going Forward: A Primer on the Encryption Debate 5,* (2016), *available at* https://homeland.house.gov/wp-content/uploads/2016/07/Staff-Report-Going-Dark-Going-Forward.pdf.

[203] Berkman Center for Internet & Society, *Don't Panic. Making Progress on the "Going Dark" Debate*, *available at* https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

[204] This suggests a role for tools that will help smaller agencies develop this expertise. *See* Edward Balkovich *et al.*, *Electronic Surveillance of Mobile Devices: Understanding the Mobile Ecosystem and Applicable Surveillance Law*, Rand Report RR800, *available at* http://www.rand.org/pubs/research_reports/RR800.html

surveillance – for either legal or technical reasons – then the department will develop a culture that not conversant with electronic surveillance.[205,206]

Finally, while this analysis has so far assumed that the interpretation of the Fourth Amendment would be shaped by the attributes of the large urban police departments that more frequently engage in electronic surveillance, it is also possible (albeit less likely) that it would instead be shaped by an event that occurred in a small town police department. Even if small town police departments adopt a particular form of electronic surveillance on a more limited basis than large urban police departments, it is possible that the actions of the small town police department would form the basis of the first case presented to an appellate court. However, a decision based on how a particular type of electronic surveillance is conducted in a small town may drastically underestimate the effects of this type of electronic surveillance in a larger community. Since the small town police departments have fewer resources and greater difficulty developing electronic surveillance expertise, the new technology may not seem like a threat to practical protections in their jurisdiction. However, the same technology could simultaneously pose a significant risk to practical protections in a larger community with greater resources and more expertise.

IV. Conclusion and Policy Recommendations

This article has described the applicable protections – both legal and practical – for individuals targeted by law enforcement surveillance. It explains how innovations in technology have undermined long-standing practical protections, and outline the arguments for expanding legal protections in order to compensate for declining practical protections. It then described variation across law enforcement agencies, focusing on differences between departments that serve large communities and those that serve small communities. It then analyzed how variation in law enforcement agencies could complicate attempts to expand legal protections in light of declining practical protections. Unless variation across different type of law enforcement agencies is taken into consideration, there may be perverse outcomes and unintended consequences.

---

[205] Anecdotally, this effect may explain difference in wiretap use across jurisdictions. Some departments in the United States – particularly those in the United States – have always been heavy users of wiretaps.

[206] That said, there may be advantages to being a late adopter of a particular form of surveillance technology. A department that adopts a particular form of surveillance later may have more information about the technical and legal challenges in using that form of surveillance. However, given that technology develops at a much quicker pace than law, a department would miss out on many benefits of technological development if they waited until the law regarding law enforcement use of a particular technology had been settled.

This article concludes by discussing several ways of addressing declining practical protections for individuals targeted by law enforcement surveillance without ignoring variation in law enforcement agencies. As will be seen, while there are no perfect solutions, there may be several ways to construct policies that account for variation across different types of law enforcement agencies.

First and foremost, the impact of law enforcement variation on the practical protections available to individuals targeted by law enforcement surveillance strongly suggests that a legislative solution would be ideal. "A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[207] While judges are limited to the case before them, legislatures can engage in extensive fact-finding and make broader rules that cover a range of situations. In particular, a legislature could request information about surveillance use from a variety of law enforcement agencies, and use that information to better characterize and regulate the barriers to electronic surveillance use. Additionally, a legislature might be better situated to balance the competing interests implicated by regulation of law enforcement surveillance, and perhaps even construct compromise solutions that leave everyone better off.

For example, a legislature could find that a particular form of electronic surveillance reduces the cost of obtaining information during criminal investigations, thus enabling law enforcement departments from large communities to gather information in a way that undermines public expectations of privacy. At the same time, however, the legislature could also find that this form of electronic surveillance is not available at all in smaller communities, which could be particularly problematic as they have fewer resources available to investigate each crime. The legislature could therefore decide to require all law enforcement agencies to obtain a warrant before using the electronic surveillance, but subsidize a training program to bring smaller law enforcement departments up to speed on how to use this form of electronic surveillance. This policy would both help protect individual rights and public safety.[208]

Additionally, legislatures may want to consider variation across different types of law enforcement departments when deciding whether and how to respond to the "going dark" debate. While the availability of encryption may make it more difficult for law enforcement to access traditional sources of information, innovations in technology may make new sources of

---

[207] *U.S. v. Jones*, 132 S. Ct. 945, 964 (2012). *See also* Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 807-8 (2004) ("Legislatures do not offer a panacea, but they do offer significant institutional advantages over courts. Legislatures can enact comprehensive rules based on expert input and can update them frequently as technology changes. As a result, legislatures can generate more nuanced, balanced, and accurate privacy rules when technology is in flux.").

[208] Furthermore, such a policy might also be more politically feasible, as it might be easier to convince decision makers to adopt a policy protecting individual rights if they can also claim to be tough on crime at the same time.

information available. However, big city police departments and small town police departments may differ in their availability to respond to these technological innovations. A legislature could elect to respond to the increase in consumer use of encryption not by requiring unwieldy and potentially risky back doors in encrypted devices,[209] but rather by assisting smaller agencies in taking advantage of those trends that are in their favor.

Although legislative action is desirable, the legislature may not choose to act. Despite (and perhaps because of) continued legislative inaction, courts will continue to be presented cases that require them to regulate criminal investigation in light of new technologies that reduce practical limitations on law enforcement surveillance. While significant challenges exist, there are several ways that the judiciary can account for variation in law enforcement agencies.

One alternative would be for judges faced with interpreting the Fourth Amendment in light of new technology to explicitly consider how practical protections for individuals targeted by surveillance have been affected in one particular type of jurisdiction. For example, judges could elect to consider the type of jurisdiction where practical protections are likely to be most affected. While such a rule would be imperfect, it would be easier to implement and lead to more consistent and predictable results across a variety of jurisdictions. However, as previously discussed,[210] ignoring variation across different types of agencies would lead to significant inefficiencies. Interpreting the Fourth Amendment too strictly could stifle the ability of law enforcement agencies in smaller jurisdictions to develop electronic surveillance capabilities; interpreting the Fourth Amendment too loosely could threaten the privacy of individuals who live in jurisdictions with particularly effective law enforcement agencies.

Another alternative would be to craft rules that explicitly take into consideration the resources of the agency conducting the search. For example, to address changes in the cost of surveillance, Bankston and Soltani (2014) advocate "a rough rule of thumb: If the cost of the surveillance using the new technique is an order of magnitude (ten time) less than the cost of the surveillance without using the new technique, then the new technique violates a reasonable expectation of privacy."[211] This metric focuses on the cost of surveillance, to the exclusion of any reference to the resources of the agency conducting the surveillance. Instead, a court could consider the decline in electronic surveillance costs relative to the resources of the law enforcement agency conducting the search.[212] To do this, the law enforcement agency that conducted the search could be required to provide documentation on the average resource expenditure per criminal investigation; one simple metric would be the ratio of operating costs to

---

[209] *See* Peter Swire and Kenesa Ahmad, *Encrpytion and Globalization*, 23 Colum. Sci. & Tech. L. Rev. 416 (2012).

[210] *See supra* section III.

[211] Bankston and Soltani, *supra* note 53, at 351.

[212] This type of fact intensive analysis would be impractical at the appellate level, but would be in line with the type of fact finding that occurs in trial courts.

criminal acts investigated. This metric could be calculated based on either the resources of the agency that conducted the search, or the resources of similarly situated agencies in the area. If the cost of surveillance has decreased from a multiple of the average resource expenditure per investigation to a fraction of the average resource expenditure per investigation, the Fourth Amendment scrutiny should apply.

However, such an approach would appear to be fundamentally unworkable. First, it would impose significant costs, both on the law enforcement agencies that would be required to provide information about their costs, and the judiciary that must weigh and analyze this evidence. Second, while the goal of this approach would be to ensure that the protections available to individuals are equal no matter where they live, it would create this equality by implementing uneven rules across different jurisdictions. These uneven rules would make it very difficult for law enforcement to anticipate which rules apply to them, and would also make it very difficult for individuals to anticipate how their information would be protected, and could raise potential equal protection issues.[213]

Finally, the fact that it is difficult to imagine a workable judicially-created rule that could account for variation across different types of law enforcement agencies suggests the difficulty of asking judges to implement empirical standards. Judicial decision makers have little ability to collect empirical evidence, and are typically tasked only with deciding the case before them. To create mechanisms for interpreting the Constitution that rely on empirical or quantitative measures seems a great departure from traditional methods of judicial decision making and can lead to significant complications, as argued above. While empirical standards can be very useful for statutory decision makers, who have the resources to collect and analyze more information, it may be too blunt an instrument for the fine-grained decisions that must be made by judges.

[213] *See*, *e.g.*, Lawrence Rosenthal, *Policing and Equal Protection*, 21 Yale L. & Pol'y Rev. 53 (2003), Carl J. Schifferle, *After* Whren v. United States*: Applying the Equal Protection Clause to Racially Discriminatory Enforcement of the Law*, 2 Mich. L. & Pol'y Rev. 159 (1997).

5. Conclusion

The primary goal of this dissertation was to describe how domestic law enforcement officers use electronic surveillance. I presented the results of three separate but related studies, each exploring a different aspect of electronic surveillance use by state and local law enforcement officers in the United States. On the whole, this work provides new, much-needed empirical evidence describing how law enforcement uses electronic surveillance. It should be useful to policymakers who are interested in crafting new laws regulating electronic surveillance, advocacy groups who are interested in proposing new electronic surveillance regulations, law enforcement officers who are interested in understanding surveillance practices from a broader perspective, and members of the general public interested in understanding how electronic surveillance is conducted and the broader effects of privacy laws.

In the first paper, I quantitatively analyzed whether state-level law enforcement use of electronic surveillance is changed by judicial rulings that affect privacy in a given state. I focused particularly on the effect of one type of judicial ruling (rejection of the third party doctrine) on one type of surveillance (wiretaps). I found that increasing legal protections for phone records decreases law enforcement use of wiretaps in a very particular way: while the number of initial requests for wiretaps remains unchanged, the number of overall requests for wiretaps and the total number of days authorized decrease. This study provides the first evidence that rejection of the third party doctrine may change how law enforcement officers conduct investigations. Since there has been increased interest in providing additional legal protections to commercially collected third party data, this research may help avoid unintended consequences.

In my second paper, I qualitatively explored how law enforcement officers use electronic surveillance and third party information requests, in order to discover the barriers to use of these techniques and identify new regulatory levers. Prior research argues that law enforcement use of surveillance has traditionally been regulated as much by practical limitations as legal limitations. Technological innovations that make it easier and cheaper for law enforcement to gather information in criminal cases therefore pose a potent threat to individual privacy, as they undermine practical limitations on investigations. By interviewing law enforcement officers who regulatory use electronic surveillance, I discovered that legal concerns and resource concerns to play a role in the decision to use electronic surveillance as well as third party information requests. However, I also identified three additional concerns that impacted this decision making process: investigatory concerns, safety concerns; and information concerns. I then describe how these concerns may represent new barriers to law enforcement use of electronic surveillance and commercial information requests, and describe the potential policy implications. I pay particular

attention to how the existence of these new barriers suggest that commercial entities are playing a considerable role in protecting the privacy of their customers against government surveillance. While there may be significant benefits in commercial entities assuming this role, as they have the resources, expertise, and perspective to serve as a meaningful check on government surveillance, there are downsides as well. In particular, since commercial entities will undoubtedly vary in their response to law enforcement in hard to observe ways, too much reliance on commercial entities may lead to uncertainties and inequities from the perspective of the consumer.

In the third paper, I described how current discussions regarding the evolving role of structural protections in regulating law enforcement surveillance are significantly complicated by variation across different types of law enforcement agencies. In particular, some academics and judges are concerned that improvements in technology may be reducing traditional, practical barriers against law enforcement surveillance; some have gone on to suggest that additional legal barriers may be necessary in their place. However, I analyze data that describes differences between police departments in large communities and police departments in small communities that that suggests the size of a police department may affect its ability to respond to changes in technology. I then argue that altering Fourth Amendment protections without taking this variation into consideration may limit the ability of smaller police departments to develop independent surveillance capabilities in a way that may undermine the balance of power between the individual and the state intended by the Fourth Amendment.

In the remainder of this section, I discuss several overarching policy concerns that arose during this research.

"Going Dark" versus the "Golden Age of Surveillance" is a False Dichotomy

Innovations in surveillance technology and the nearly ubiquitous nature of commercial data collection have created new sources of information that law enforcement can draw on – often with minimal legal protections. Accordingly, some scholars have persuasively argued that we are now in a "golden age of surveillance": an era in which "investigatory agencies have unprecedented access to information about a suspect."[214] On the other hand, some law enforcement agencies have demonstrated that certain sources of information traditionally available to law enforcement can no longer be accessed due to the adoption of encryption technology. These sources of information are described as "going dark": even though law enforcement is able to obtain an appropriate legal order, they "often lack[] the technical ability to

[214] *See*, *e.g.*, Peter Swire and Kenesa Ahmad, *Encryption and Globalization*, 13 Colum. Sci. & Tech L. Re. 416, 470 (2012).

carry out those orders because of a fundamental shift in communications services and technologies."[215]

These two descriptions of the state of electronic surveillance are frequently implicitly and explicitly discussed in competing terms. For example, in a recent interview with Time Magazine, Tim Cook described the going dark problem as "a crock": even though encryption may prevent law enforcement from accessing some narrow domains of data, "we shouldn't all be fixated just on what's not available…[b]ecause there's a mountain of information about us. I mean there's so much...it's a mountain of data."[216] In contrast, FBI Director James Comey has argued that the metadata collected by commercial entities are not a replacement for the information lost to encryption. According to Director Comey, commercial metadata is "incomplete information, and even this is difficult to access when time is of the essence. I wish we had time in our work, especially when lives are on the line. We usually don't."[217]

However, this is a false dichotomy. It is entirely possible – and indeed plausible – that we are in both a golden age of surveillance and law enforcement is experiencing a problem with surveillance going dark. While technological innovation has made it significantly easier for law enforcement to obtain certain types of information from commercial entities, other forms of information (particularly the contents of now-encrypted communication) are becoming difficult – if not impossible – to access. Furthermore, as is evidenced by the research in this dissertation, different types of law enforcement agencies face different constraints. The increased availability of commercially collected data may bring on a golden age for those large city police departments that can fully take advantage of it, while police departments that serve smaller localities may be stuck in the dark, as they simultaneously lose traditionally available forms of surveillance and are unable to fully take advantage of new sources of information.

Electronic Surveillance Policy is Not Just a Numbers Game

Related to the conversation about going dark vs. golden age, electronic surveillance is often discussed in terms of "too much" or "not enough." Indeed, what little empirical evidence is available suggests that electronic surveillance use is increasing.[218] However, the mere fact that

---

[215] *See*, *e.g.*, Federal Bureau of Investigation, *Going Dark Issue*, https://www.fbi.gov/about-us/otd/going-dark-issue

[216] Nancy Gibbs and Lev Grossman, *Here's the Full Transcript of TIME's Interview With Apple CEO Tim Cook*, http://time.com/4261796/tim-cook-transcript/.

[217] James B. Comey, *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?*, *Remarks to the Brookings Institution*, https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course (last visited Sept. 15, 2016).

[218] *See*, *e.g.*, Google, *Transparency Report*, *available at* https://www.google.com/transparencyreport/.

electronic surveillance use is rising provides little information about whether it is being used in a way that threatens privacy rights. Electronic surveillance is a powerful law enforcement technique that can protect public safety in an effective and cost efficient manner.[219] Like any investigative technique, electronic surveillance poses a threat to Constitutional rights if abused. But use – even increasingly frequent use – is not the same as abuse. Representatives from the law enforcement community have argued that the increased number of electronic surveillance requests is not due to an increase in the prevalence of surveillance, but rather due to changes in communication patterns and the utilization of counter-surveillance practices by criminal entities.[220] Without additional context, the number of electronic surveillance requests alone does not provide policy makers with the information necessary to regulate law enforcement practices.

As is evidenced by my research, regulation of one form of surveillance may impact law enforcement's ability to utilize other forms of surveillance. For example, I demonstrated that more tightly regulating law enforcement access to phone records decreases the duration of their use of wiretaps. This research suggests that discussions of how law enforcement phone records should be regulated should include a discussion of how these regulations will affect wiretaps. This discussion of downstream effects will help avoid unintended effects on other forms of surveillance.

My goal in conducting this research is to shift the conversation around how surveillance should be regulated, not to advocate for a particular perspective. I believe the results of my research could be used by either a public safety advocate or a privacy advocate. A public safety advocate could use my work to argue that law enforcement access to phone records should not be restricted, since it would negatively impact law enforcement's ability to use other important surveillance tools. However, a privacy advocate could argue that restricting law enforcement access to phone records will have an additional, beneficial effect of helping to limit the duration of law enforcement use of more invasive surveillance mechanisms. Regardless of the point of view, however, the conversation will be focused on how the surveillance mechanism is used in practice, and based on empirical evidence.

---

[219] Samuel Nunn, *Measuring criminal justice technology outputs: The case of Title III wiretap productivity, 1987-2005*, 36 J. Crim. Just. 344 (2008).

[220] Mark D. Young, *Electronic surveillance in an era of modern technology and evolving threats to national security*, 22 Stan. L. & Pol'y Rev. 11 (2011).

Appendix A. Bibliography, Does Rejection of the Third Party Doctrine Change Use of Electronic Surveillance?

Case Law

Katz v. United States, 389 U.S. 347 (1967).
Chimel v. California, 395 U.S. 752 (1969).
United States v. Matlock, 415 U.S. 164 (1973).
United States v. Milledr, 426 U.S. 435 (1976).
Smith v. Maryland, 442 U.S. 735 (1978).
Payton v. New York, 445 U.S. 573 (1980).
United States v. Knotts, 460 U.S. 276 (1983).
People v. Sporleder, 666 P.2d 135 (Colo. 1983).
Oliver v. United States, 466 U.S. 170 (1984).
Arizona v. Hicks, 480 U.S. 321 (1986).
United States v. Jones, 132 S.Ct. 945 (2012).

Constitutional and Statutory Law

1791. U.S. Const. Amend. IV.
2015. 18 U.S.C. Sec. 2519
2015. Arizona Revised Statutes 13-3010, 13-3017.
2015. Colorado Revised Statutes 16-15-102.

Books and Articles

Amar, Akhil Reed. 1994. "Fourth Amendment First Principles." *Harvard Law Review* 107 (4): 757. doi:10.2307/1341994.

Bankston, Kevin S, and Ashkan Soltani. 2014. "Tiny Constables and the Cost of Surveillance: Making Cents Out of *United States v. Jones*." *The Yale Law Journal* 123: 335.

Bertrand, Marianne, Esther Duflo, and Sendhil Mullainathan. 2002. "How Much Should We Trust Differences-in-Differences Estimates?." Cambridge, MA: National Bureau of Economic Research. doi:10.3386/w8841.

Conley, Timothy G, and Christopher R Taber. 2011. "Inference with 'Difference in Differences' with a Small Number of Policy Changes." *Review of Economics and Statistics* 93 (1): 113–25. doi:10.1162/REST_a_00049.

Dash, Samuel. 1971. *The Eavesdroppers*. New York: Da Capo Press.

Henderson, S E. 2011. "The Timely Demise of the Fourth Amendment Third Party Doctrine." *Iowa L Rev Bull* 96: 39.

Henderson, Stephen E. 2006. “Learning From All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information From Unreasonable Search” 55 (2): 373.
Henderson, Stephen E. 2013. “After *United States v. Jones*, After the Fourth Amendment Third Party Doctrine.” *SSRN Electronic Journal*. doi:10.2139/ssrn.2195274.
Kane, Robert J. 1999. “Patterns of Arrest in Domestic Violence Encounters: Identifying a Police Decision-Making Model.” *J. Crim. Just.* 27 (1): 65–79.
Kerr, Orin S. 2001. “The Fourth Amendment in Cyberspace: Can Encryption Create a ‘Reasonable Expectation of Privacy?’” 33: 503.
Kerr, Orin S. 2004. “The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution.” *Michigan Law Review* 102 (5): 801. doi:10.2307/4141982.
Kerr, Orin S. 2007. “Four Models of Fourth Amendment Protection.” *Stanford Law Review* 60 (2): 503.
Kerr, Orin S. 2009. “The Case for the Third-Party Doctrine.” *Michigan Law Review* 107 (4): 561–601.
Ku, Raymond Shih Ray. 2002. “The Founders' Privacy: the Fourth Amendment and the Power of Technological Surveillance.” *Minn. L. Rev.* 86 (6). University of Chicago Press: 1325–78. doi:10.7208/chicago/9780226762944.003.0002.
Lammon, Bryan D. 2007. “The Practical Mandates of the Fourth Amendment: a Behavioral Argument for the Exclusionary Rule and Warrant Preference.” *Washington University Law Review* 85: 1101.
Marcus, Paul, Melanie D Wilson, and Jack B Zimmermann. 2014. *Criminal Procedure in Practice*. Fourth Edition. American Bar Association Criminal Justice Section.
Mason, Caleb. 2012. “New Police Surveillance Technologies and the Good-Faith Exception: Warrantless GPS Tracker Evidence After *United States v. Jones*.” *Nevada Law Journal* 13: 60.
Minzner, Max, and Christopher M Anderson. 2013. “Do Warrants Matter?.” *Review of Law & Economics* 9 (2): 169–96. doi:10.1515/rle-2012-0027.
Nunn, Samuel. 2008. “Measuring Criminal Justice Technology Outputs: the Case of Title III Wiretap Productivity, 1987-2005.” *Journal of Criminal Justice* 36 (4): 344–53. doi:10.1016/j.jcrimjus.2008.06.006.
Owsley, Brian L. 2013. “The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance” 16: 1.
Phillips, Scott W, and James J Sobol. 2010. “Twenty Years of Mandatory Arrest: Police Decision Making in the Face of Legal Requirements.” *Criminal Justice Policy Review* 21 (1): 98–118. doi:10.1177/0887403408322962.
Ridgeway, Greg. 2007. “Analysis of Racial Disparities in the New York Police Department's Stop, Question, and Frisk Practices.” *RAND Report*.
Schafer, Joseph A, David L Carter, Andra J Katz-Bannister, and William M Wells. 2006. “Decision Making in Traffic Stop Encounters: a Multivariate Analysis of Police Behavior.” *Police Quarterly* 9 (2): 184–209. doi:10.1177/1098611104264990.
Shocker, Allan D, Barry L Bayus, and Namwoon Kim. 2004. “Product Complements and Substitutes in the Real World: the Relevance of ‘Other Products’.” *J. Marketing* 68 (1): 28–40.
Slobogin, Christopher, and Joseph E Schumacher. 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. doi:10.2307/1372714.
Smith, Michael R, and Matthew Petrocelli. 2001. "Racial Profiling? a Multivariate Analysis of Police Traffic Stop Data." *Police Quarterly* 4 (1): 4–27.
Solove, D J. 2006. "A Brief History of Information Privacy Law." *Proskauer on Privacy*. doi:10.1201/9781420031256.ch1.
Terrill, William, and Stephen D Mastrofski. 2002. "Situational and Officer-Based Determinants of Police Coercion." *Justice Quarterly* 19 (2): 215–48. doi:10.1080/07418820200095221.
The Berkman Center. 2016. "Don't Panic: Making Progress on the "Going Dark" Debate."
Tokson, Matthew J. 2009. "The Content/Envelope Distinction in Internet Law." *Wm. Mary L. Rev.* 50: 2105.
1791. *U.S. Const. Amend. IV*.
1902. "State Constitutions and the Protection of Individual Rights." *Harvard Law Review* 16 (1): 58. doi:10.2307/1322517.
1927. Olmstead et al. v. United States, 277 U.S. 438.
1937. "*Nardone v. United States*." *U.S.* 302: 379.
1961a. "Mapp v. Ohio." *U.S.* 367: 643.
1961b. "Silverman Et Al. v. United States." *U.S.* 365: 505.
1967. "Katz v. United States." *U.S.* 389: 347.
1968a. "Alderman v. United States." *U.S.* 394: 165.
1968b. "Chimel v. California." *U.S.* 395: 752.
1973. "United States v. Matlock." *U.S.* 415: 164.
1976. "United States v. Miller." *U.S.* 425: 435.
1978. "Smith v. Maryland." *U.S.* 442: 735.
1980. "Payton v. New York." *U.S.* 445: 573.
1983a. "Illinois v. Gates." *U.S.* 462: 213.
1983b. "United States v. Knotts." *U.S.* 460: 276.
1984a. "Oliver v. United States." *U.S.* 466: 170.
1984b. "United States v. Karo." *U.S.* 468: 705.
1986. "Arizona v. Hicks." *U.S.* 480: 321.
1998. *Privacy on the Line*. Vol. 35. Choice Reviews Online. doi:10.5860/CHOICE.35-6456.
2000. "Kyllo v. United States." *U.S.* 533: 27.
2005. "Widgren v. Maple Grove Township." *F.D* 429: 575.
2012. "United States v. Jones." *S. Ct.* 132: 945.
2015a. *18 U.S.C. Sec. 2510*.
2015b. "Fourth Amendment."
n.d. *18 U.S.C. Sec. 2511, 2015*.
n.d. *18 U.S.C. Sec. 2516, 2015*.
n.d. *18 U.S.C. Sec. 2518, 2015*.
n.d. *18 U.S.C. Sec. 2519, 2015*.
n.d. *18 U.S.C. Sec. 3123, 2015*.
n.d. *Cal. Pen. Code. Sec. 631*.
n.d. *Mont. Code. Ann. Sec. 45-8-213*.
n.d. People v. McGee, 49 N.Y. 2d 48.
n.d. *Tex. Pen. Code Ann. Sec. 16.02*.

Appendix B. Description of State Supreme Court Cases Affirming or Rejecting the Third-Party Doctrine

This appendix comprises three separate tables, each describing state supreme court cases that rejected the third-party doctrine with respect to a particular type of information. For each case, a brief quote stating the holding is provided.

Phone Records

Table B.1. State Case Law Related to the Application of the Third Party Doctrine to Phone Records

State	Case Name	Citation	Year	TPD Rejected?	Supporting Language
Maryland	*Smith v. State*	283 Md. 156	1978	No	"We hold that there is no constitutionally protected reasonable expectation of privacy in the numbers dialed into a telephone system and hence no search within the fourth amendment is implicated by the use of a pen register installed at the central offices of the telephone company."
California	*People v. Blair*	25 Cal. 3d 640	1979	Yes	"Thus, if, as we shall conclude, the rationale of Burrows applies to the records of the credit card charges made by defendant, the prosecution did not lawfully obtain those records."
Indiana	*In re Order for Indiana Bell Tel. to Disclose Records*	274 Ind. 131	1980	No	"Indiana Bell argues that extra-judicial intrusion by law enforcement authorities in the records of telephone communications impermissibly infringes upon the freedoms of speech and association guaranteed under the State and Federal Constitutions. We do not agree...The expectation of privacy protected by the Fourth Amendment attaches to the content of the telephone conversation and not to the fact that a conversation took place."

State	Case Name	Citation	Year	TPD Rejected?	Supporting Language
Montana	*Hastetter v. Behan*	196 Mont. 280	1982	No	"Likewise, the Montana constitutional provision protecting an individual's right of privacy protects only matters which can reasonably be considered private. Telephone company billing records are not private matters. "
New Jersey	*State v. Hunt*	91 N.J. 338	1982	Yes	"In this case we are persuaded that the equities so strongly favor protection of a person's privacy interest that we should apply our own standard rather than defer to the federal provision."
New York	*People v. Di Raffaele*	55 N.Y.2d 234	1982	No	"Defendant had no legitimate expectation of privacy in the records maintained by the telephone company with respect to either his own telephone or that of his friend, and their release to the District Attorney of Suffolk County worked no violation of defendant's right to be free from unreasonable searches and seizures under the Fourth Amendment to the Federal Constitution.... We decline defendant's invitation to establish a more restrictive standard under the provisions of section 12 of article I of the New York State Constitution, concluding that there is no sufficient reason for any such differentiation..."
Colorado	*People v. Sporleder*	666 P.2d 135	1983	Yes	"The People's principal argument is that the defendant had no legitimate expectation of privacy in the telephone numbers she dialed on her home telephone and, hence, the warrantless installation of the pen register did not violate the Colorado constitutional prohibition against unlawful searches and seizures. We disagree."
California	*People v. Chapman*	36 Cal. 3d 98	1984	Yes	"The holdings in Burrows and Blair compel one conclusion — that respondent McGee demonstrated a reasonable expectation of privacy in her unlisted name, address, and telephone number."
Colorado	*People v. Corr*	682 P.2d 20	1984	Yes	"The prosecution would distinguish between pen registers, which record all telephone numbers dialed from a specific telephone, and toll records, which record only those calls individually billed, because of an asserted lesser expectation of privacy in the latter. We reject this distinction. It is clear from the rationale of Sporleder that individually billed calls enjoy the same expectation of privacy as other calls do. "

State	Case Name	Citation	Year	TPD Rejected?	Supporting Language
Delaware	*Gibbs v. State*	479 A.2d 266	1984	No	"We find that defendant's concern is misplaced in that Fourth Amendment protection is not invoked unless there is a reasonable or legitimate expectation of privacy.... Applying this standard, the defendant cannot have a legitimate expectation of privacy in his toll call records in that this information is voluntarily conveyed to the phone company, which retains this information for billing purposes. Therefore, as in the case of a pen register, no warrant is required."
New York	*People v. Guerra*	65 N.Y.2d 60	1985	No	"In each instance, however, the information is available to the telephone company and, as we noted in People v Di Raffaele (supra), the defendant "had no legitimate expectation of privacy in the records maintained by the telephone company"."
Washington	*State v. Gunwall*	106 Wn.2d 54	1986	Yes	"Based on the foregoing, we conclude that when the police obtained the defendant's long distance telephone toll records, and when they placed a pen register on her telephone line or connections, all without benefit of the issuance of any valid legal process, they unreasonably intruded into her private affairs without authority of law and in violation of Washington Const. art. 1, § 7."
New Hampshire	*State v. Valenzuela*	130 N.H. 175	1987	No	"Under Katz and the agent-informer cases, there is no violation of constitutional privacy when the telephone operator acts as a government informer by communicating what a defendant has addressed to the operator, and we therefore find no violation when the "hearer" is not an operator, but a machine receiving functionally equivalent information communicated by a defendant and directed to the company."
Florida	*Shaktman v. State*	553 So.2d 148	1989	Yes	"We agree with the district court that the compelling state interest test articulated in Winfield must be applied to the issue before us. Because the pen register intrudes upon fundamental privacy interests, the state has the burden of demonstrating both that the intrusion is justified by a compelling state interest and that the state has used the least intrusive means in accomplishing its goal."

State	Case Name	Citation	Year	TPD Rejected?	Supporting Language
Hawaii	*State v. Rothman*	70 Haw. 546	1989	Yes	"We agree with the trial judge that persons using telephones in the State of Hawaii have a reasonable expectation of privacy, with respect to the telephone numbers they call on their private lines, and with respect to the telephone numbers of calls made to them on their private lines. That is, they have a reasonable expectation that the government will not tap their private telephones to obtain such information, or require the telephone company to supply such information to it, unless the government has obtained a proper and legal warrant therefor."
Idaho	*State v. Thompson*	114 Idaho 746	1989	Yes	"We hold that the use of a pen register is a search under art. 1, § 17 of the Idaho Constitution, that the evidence produced by the pen register should not have been considered in the issuance of the wiretap orders, and that without the pen register evidence there was no probable cause to issue the wiretap orders."
New Jersey	*State v. Mollica*	114 N.J. 329	1989	Yes	"We conclude that the state constitutional prohibition against unreasonable search and seizure applies to an individual's hotel telephone billing records based on his or her use of a hotel-room telephone. We find nevertheless that when such telephone records are seized by federal officers acting independently of state authorities and in conformity with federal law, this state constitutional protection does not bar subsequent prosecutorial use of those records for such purposes as establishing probable cause for the issuance of search warrants."
Pennsylvania	*Commonwealth v. Melilli*	521 Pa. 405	1989	Yes	"We also determine as part of this analysis that the installation of pen registers must be supported by probable cause."
Kansas	*State v. Schultz*	252 Kan. 819	1993	No	"We are persuaded by the reasoning in Miller and Smith that, because the bank and telephone customer knows and understands others will see the records, the customer should have no expectation of privacy."
Wyoming	*Saldana v. State*	846 P.2d 604	1993	No	"The fact that Saldana's telephone number was not listed, even though permitting increased expectation of privacy with respect to who might call him, is a distinction without a difference for the purposes of this case. Here there was no "search" that invaded a legitimate expectation of privacy and, for that reason, no warrant was required."

State	Case Name	Citation	Year	TPD Rejected?	Supporting Language
Ohio	*Ohio Domestic Violence Network v. Pub. Util. Comm.*	70 Ohio St. 3d 311	1994	No	"We find Smith controlling as to appellants' Fourth Amendment claim." "We have recognized that this provision is virtually identical to the Fourth Amendment to the federal Constitution and refuse to impose greater restrictions under it."
Massachusetts	*Commonwealth v. Raymond P. Vinnie*	428 Mass. 161	1998	No	"For the reasons set forth by the Appeals Court, Vinnie's constitutional attack on the statute also fails."
Colorado	*People v. Mason*	989 P.2d 757	1999	Yes	"We now hold that a subpoena duces tecum for such records is not an unreasonable search and seizure under Article II, Section 7 of the Colorado Constitution provided that it is supported by probable cause and is properly defined and executed"
New Hampshire	*State v. Gubitosi*	152 N.H. 673	2005	No	"We decline the defendant's invitation to overrule Valenzuela...As discussed above, the defendant did not have a reasonable expectation of privacy in the records obtained from U.S. Cellular. "

Business Records

Table B.2. State Case Law Related to the Application of the Third Party Doctrine to Business Records

State	Case Name	Citation	Year	TPD Rejected?	Supporting Language
California	*Burrows v. Superior Court*	529 P.2d 590	1974	Yes	"We hold that any bank statements or copies thereof obtained by the sheriff and prosecutor without the benefit of legal process were acquired as the result of an illegal search and seizure (Cal. Const., art. I, § 13), and that the trial court should have granted the motion to suppress such documents."
Pennsylvania	*Commonwealth v. De John*	486 Pa. 32	1979	Yes	"We are convinced that under Art. I, § 8, of the Pennsylvania Constitution bank customers have a legitimate expectation of privacy in records pertaining to their affairs kept at the bank"
Wyoming	*Fitzgerald v. State*	599 P.2d 572	1979	No	"With respect to the points of error arising out of the obtaining of the bank records and the United States Postal Service records without legal process, we note the holding of the Supreme Court of the United States in United States v. Miller, 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976), to the effect that a person has no reasonable expectation of privacy with respect to bank records....The permission of the bank to search for the records was deemed to be adequate for the officers to obtain them. We adopt this rule and in so doing reject the contrary rule espoused by the California court in Burrows v. Superior Court of San Bernardino County, 13 Cal.3d 238, 118 Cal. Rptr. 166, 529 P.2d 590 (1975)."
Colorado	*Charnes v. Digiacomo*	200 Colo. 94	1980	Yes	"We agree with the taxpayer that he has an expectation of privacy in his bank records and that the records are protected from unreasonable search and seizure by the Department of Revenue."
Pennsylvania	*Commonwealth v. Murtha*	475 A.2d 783	1984	Yes	"These consolidated, direct appeals raise an issue of first impression in this Commonwealth: whether the utilization by law enforcement agencies of pen registers or dialed number recorders (DNRs) requires a judicial order based upon probable cause. We hold that such an order is required, and reverse the judgments of sentence."

State	Case Name	Citation	Year	TPD Rejected?	Supporting Language
Florida	*Winfield v. Division of Pari-Mutuel Wagering*	477 So. 2d 544	1985	Yes	"[W]e hold that article I, section 23, of the Florida Constitution does not prevent the Division of Pari-Mutuel wagering from subpoenaing a Florida citizen's bank records without notice."
Hawaii	*State v. Klattenhoff*	71 Haw. 598	1990	No	"Although a minority of states have held, as a matter of state constitutional law, that there is a reasonable expectation of privacy in bank records, we do not find that the Hawaii Constitution provides such a right. Therefore, we adopt the rule set forth in United States v. Miller, and follow the majority of states in finding no reasonable expectation of privacy in personal bank records."
Utah	*State v. Thompson*	810 P.2d 415	1991	Yes	"We hold that under article I, section 14 of the Utah Constitution, defendants under the facts of this case had a right to be secure against unreasonable searches and seizures of their bank statements, "checks, savings, bonds, loan applications, loan guarantees, and all papers which [they] supplied to the bank to facilitate the conduct of [their] financial affairs upon the reasonable assumption that the information would remain confidential.""
Kansas	*State v. Schultz*	252 Kan. 819	1993	No	"We are persuaded by the reasoning in Miller and Smith that, because the bank and telephone customer knows and understands others will see the records, the customer should have no expectation of privacy."
New Jersey	*State v. McAllister*	184 N.J. 17	2005	Yes	"We hold that, under the New Jersey Constitution, citizens have a reasonable expectation of privacy in bank records."
Washington	*State v. Miles*	160 Wn.2d 236	2007	Yes	"Private bank records may disclose what the citizen buys, how often, and from whom. They can disclose what political, recreational, and religious organizations a citizen supports. They potentially disclose where the citizen travels, their affiliations, reading materials, television viewing habits, financial condition, and more. Little doubt exists that banking records, because of the type of information contained, are within a person's private affairs."
North Dakota	State v. Hammer	2010 ND 152	2010	No	"We hold the district court did not err by denying Hammer's motion to suppress bank records obtained through administrative subpoenas duces tecum, denying Hammer's motions to dismiss on double jeopardy grounds, or permitting the State to file an amended information. "

Location Information

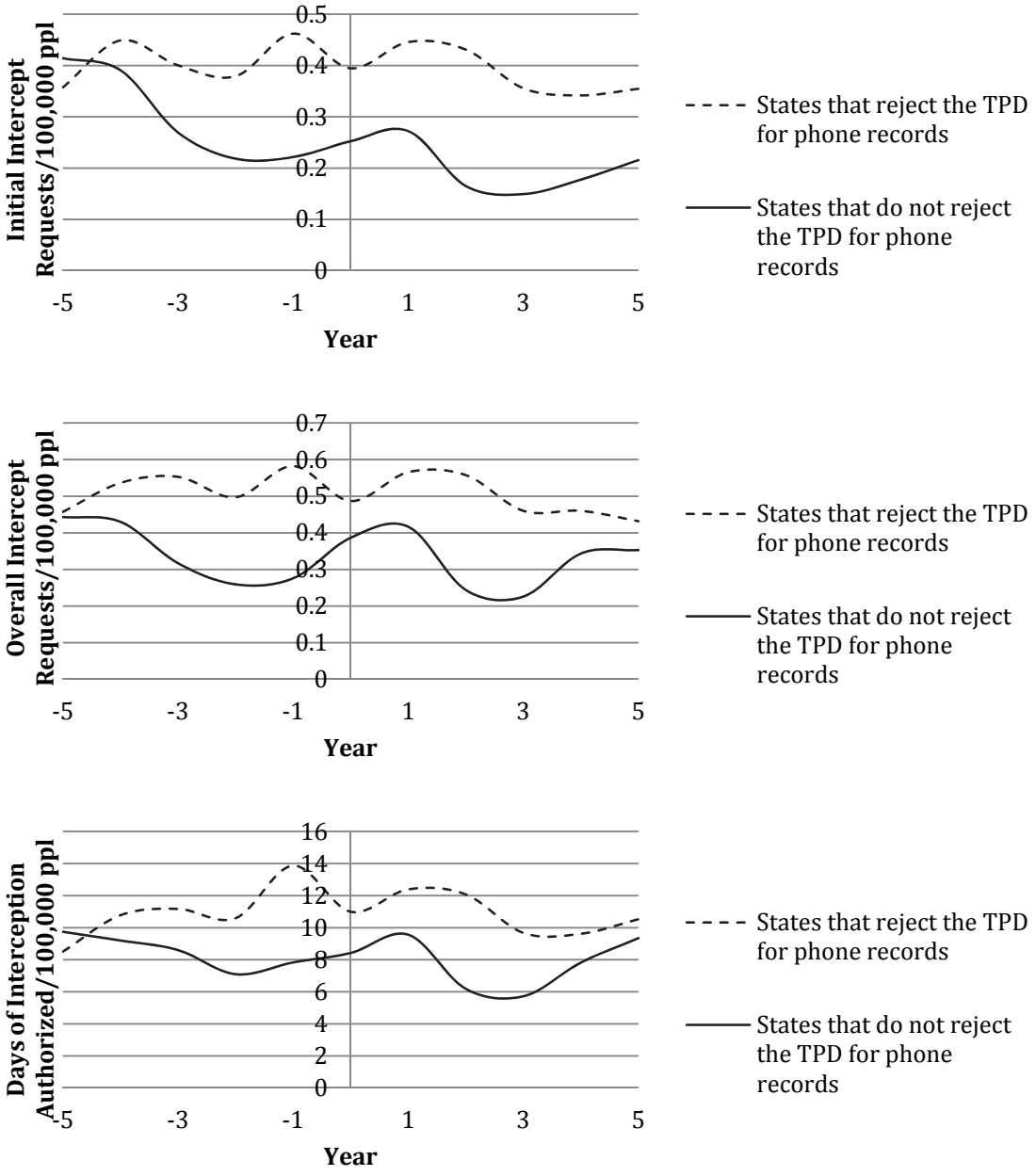
Table B.3. State Case Law Related to the Application of the Third Party Doctrine to Location Information

State	Case Name	Citation	Year	TPD Rejected?	Supporting Language
Colorado	*People v. Oates*	698 P.2d 811	1985	Yes	"We conclude that the broader definition of what constitutes a legitimate expectation of privacy under the Colorado Constitution encompasses the expectation that purchased commercial goods will be free of government surveillance devices such as beepers. We therefore depart from the reasoning in Karo and hold that the installation and continued presence of the beeper in this case infringed upon the legitimate expectations of privacy of at least one defendant, and therefore constituted a search requiring a warrant under article II, section 7 of the Colorado Constitution."
Oregon	*State v. Campbell*	306 Ore. 157	1988	Yes	"The issue is whether police use of a radio transmitter to locate a private automobile to which the transmitter has been surreptitiously attached is a "search" or "seizure" under Article I, section 9, of the Oregon Constitution.[1] We hold that it is a search. Because no warrant authorized the police to locate defendant's automobile in this manner, we affirm the decisions of the circuit court and the Court of Appeals to suppress the evidence thereby obtained."
Nevada	*Osburn v. Nevada*	44 P.3d 523	2002	No	"[T]he attachment of the electronic tracking device to the bumper of Osburn's vehicle did not constitute an unreasonable search or seizure under the Nevada Constitution."
Washington	*State v. Jackson*	76 P.3d 217	2003	Yes	"We conclude that citizens of this State have a right to be free from the type of governmental intrusion that occurs when a GPS device is attached to a citizen's vehicle, regardless of reduced privacy expectations due to advances in technology. We hold that under article I, section 7 a warrant is required for installation of these devices."

State	Case Name	Citation	Year	TPD Rejected?	Supporting Language
Massachusetts	Commonwealth v. Connolly	454 Mass. 808	2009	Yes	"We conclude that . . . the use of a GPS tracking device requires a warrant for purposes of art. 14 of the Massachusetts Declaration of Rights"
New York	People v. Weaver	12 N.Y.3d 433	2009	Yes	"The massive invasion of privacy entailed by the prolonged use of the GPS device was inconsistent with even the slightest reasonable expectation of privacy."

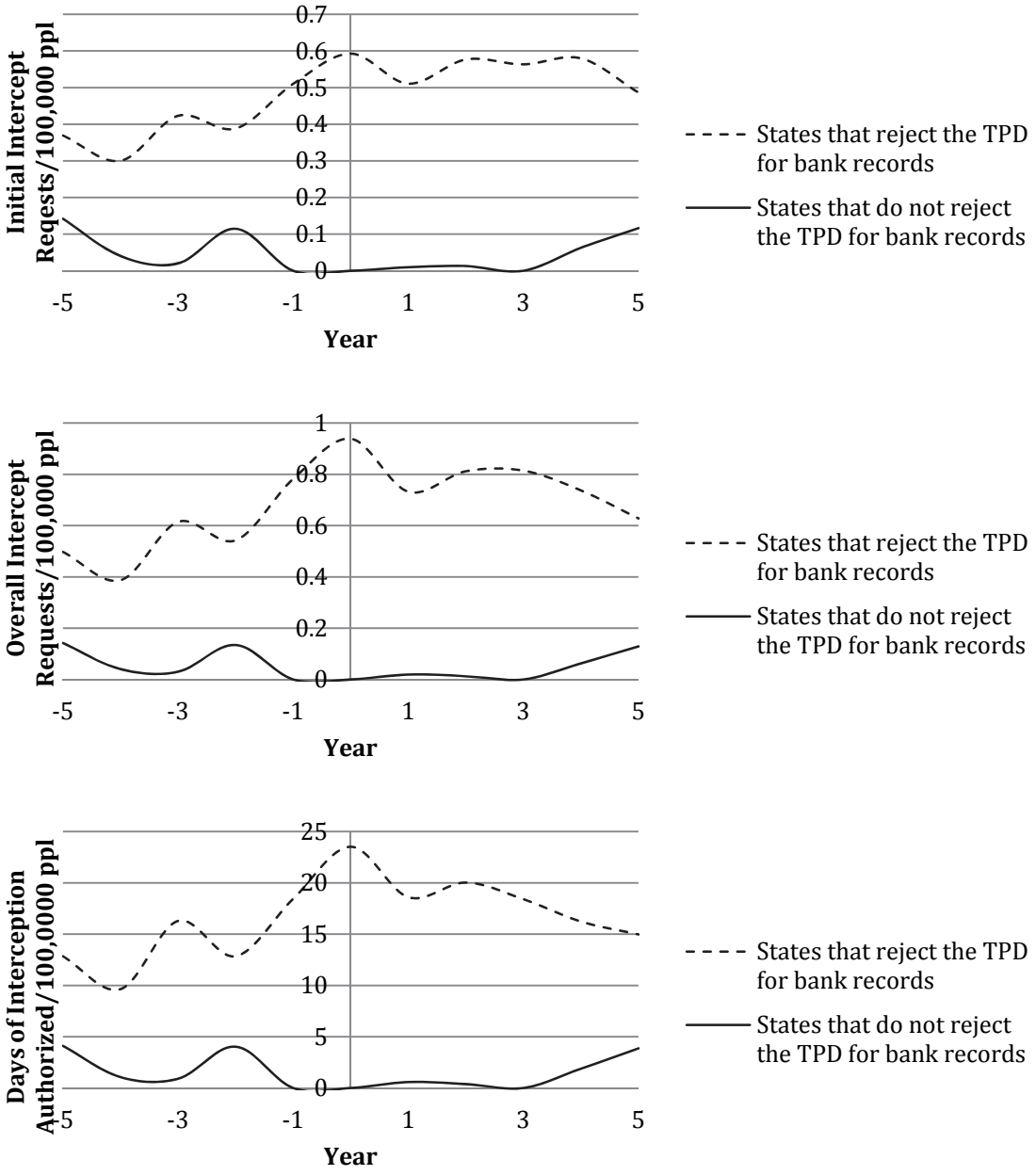
Appendix C. Additional Comparison of Intercept Trends

Figure C.1. Comparing Trends in Intercept Use, Phone Records



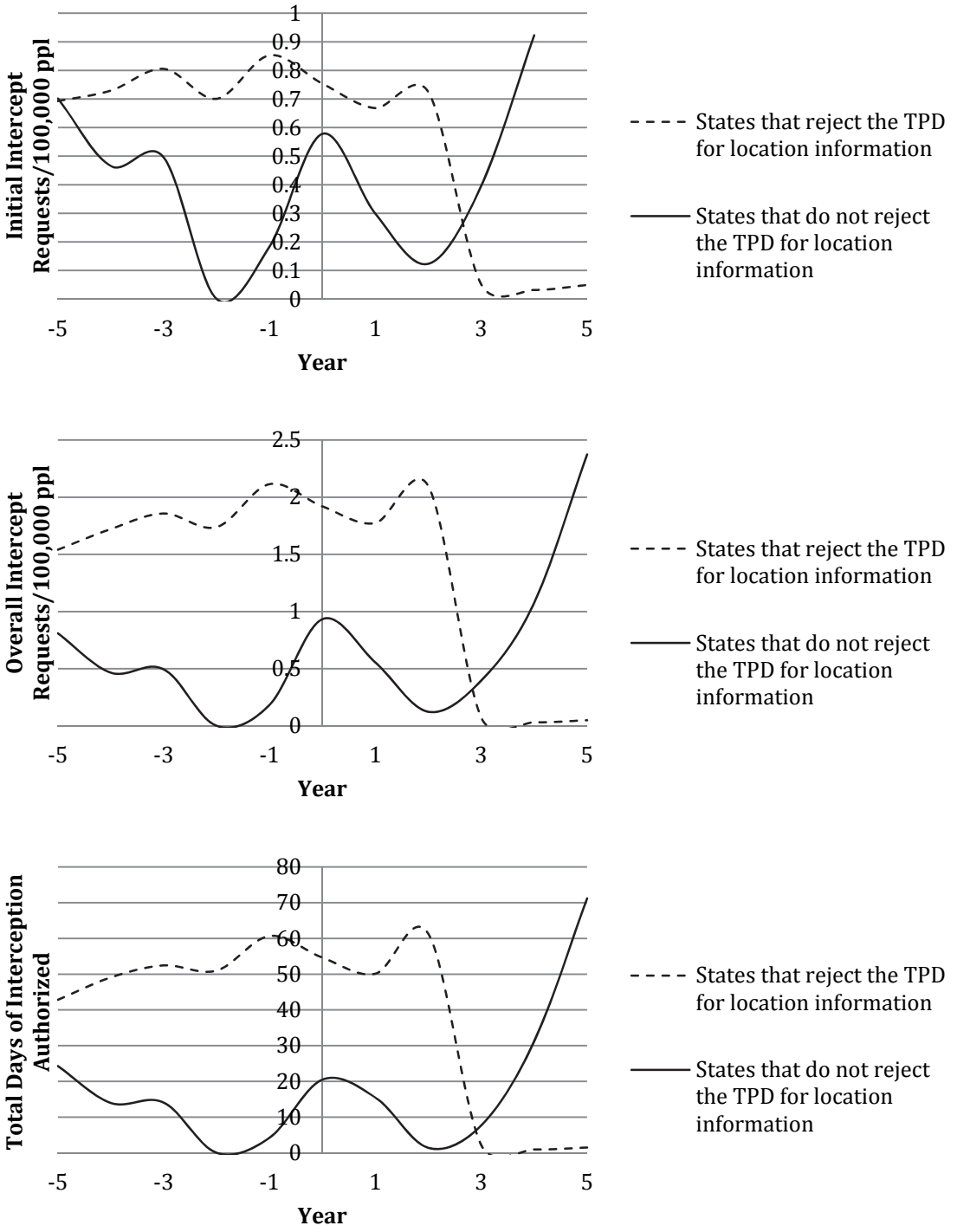
These charts describe trends in metrics of intercept use by state-level law enforcement before and after state supreme court opinions related to the third party doctrine. Year 0 corresponds to the year in which the opinion was decided. Separate trend lines are presented for states that reject and do not reject third party doctrine with regards to phone records information.

Figure C.2. Comparing Trends in Intercept Use, Bank Records



These charts describe trends in metrics of intercept use by state-level law enforcement before and after state supreme court opinions related to the third party doctrine. Year 0 corresponds to the year in which the opinion was decided. Separate trend lines are presented for states that reject and do not reject third party doctrine with regards to bank records information.

Figure C.3. Comparing Trends in Intercept Use, Location Information



These charts describe trends in metrics of intercept use by state-level law enforcement before and after state supreme court opinions related to the third party doctrine. Year 0 corresponds to the year in which the opinion was decided. Separate trend lines are presented for states that reject and do not reject third party doctrine with regards to location information.

Appendix D. Results of Sensitivity Analyses

Table D.1A. Effect of Rejecting the Third Party Doctrine on Number of Initial Intercept Requests, Including Statutory Law

	(I)	*(I)*	*(I)*	(II)	(II)	(II)
Any Rejection of TPD	-0.115	-0.353*	-0.193			
	(0.192)	(0.198)	(0.137)			
Rejection of TPD for Phone Records				-0.162	-0.401*	-0.306
				(0.225)	(0.235)	(0.186)
Rejection of TPD for Bank Records				-0.162	-0.321	-0.061
				(0.202	(0.218)	(0.145)
Rejection of TPD for Location Info				0.082	-0.275	-0.212
				(0.331)	(0.356)	(0.178)
Policy Controls	Y	Y	Y	Y	Y	Y
Urban Arrest Controls	N	Y	Y	N	Y	Y
Crime Controls	N	N	Y	N	N	Y
Demo Controls	N	N	Y	N	N	Y
Urbanicity Control	N	N	Y	N	N	Y
Year Fixed Effects	Y	Y	Y	Y	Y	Y
State Fixed Effects	Y	Y	Y	Y	Y	Y
N	1640	1383	1383	1640	1383	1383

This table provides the results of difference-in-difference analyses estimating the effects of rejecting the third party doctrine on the number of requests for communication intercepts made per 100,000 people in a given state in a given year. A Poisson regression model was used, and robust standard errors were used to account for clustering at the state level. State and year fixed effects were included on all regressions. *** denotes statistical significance at the 0.01 level; ** denotes statistical significance at the 0.05 level; *** denotes statistical significances at the 0.1 level.

Table D.1B. Effect of Rejecting the Third Party Doctrine on Overall Number of Wiretap Requests, Including Statutory Law

	(III)	(III)	(III)	(IV)	(IV)	(IV)
Any Rejection of TPD	-0.211	-0.418**	-0.282**			
	(0.177)	(0.169)	(0.121)			
Rejection of TPD for Phone Records				-0.408	-0.627**	-0.478**
				(0.269)	(0.270)	(0.192)
Rejection of TPD for Bank Records				-0.207	-0.351*	-0.179
				(0.190)	(0.194)	(0.146)
Rejection of TPD for Location Info				0.114	-0.071	-0.048
				(0.266)	(0.322)	(0.188)
Policy Controls	Y	Y	Y	Y	Y	Y
Urban Arrest Controls	N	Y	Y	N	Y	Y
Crime Controls	N	N	Y	N	N	Y
Demo Controls	N	N	Y	N	N	Y
Urbanicity Control	N	N	Y	N	N	Y
Year Fixed Effects	Y	Y	Y	Y	Y	Y
State Fixed Effects	Y	Y	Y	Y	Y	Y
N	1640	1383	1383	1640	1383	1383

This table provides the results of difference-in-difference analyses estimating the effects of rejecting the third party doctrine on the number of requests for communication intercepts made per 100,000 people in a given state in a given year. A Poisson regression model was used, and robust standard errors were used to account for clustering at the state level. State and year fixed effects were included on all regressions. *** denotes statistical significance at the 0.01 level; ** denotes statistical significance at the 0.05 level; *** denotes statistical significances at the 0.1 level.

Table D.1C. Effect of Rejecting the Third Party Doctrine on Total Days of Interception Authorized, Including Statutory Law

	(V)	(V)	(V)	(VI)	(VI)	(VI)
Any Rejection of TPD	-0.285	-0.505***	-0.306***			
	(0.176)	(0.163)	(0.114)			
Rejection of TPD for Phone Records				-0.510*	-0.759***	-0.551***
				(0.267)	(0.264)	(0.186)
Rejection of TPD for Bank Records				-0.253	-0.419**	-0.170
				(0.194)	(0.184)	(0.134)
Rejection of TPD for Location Info				-0.028	-0.212	-0.111
				(0.267)	(0.305)	(0.180)
Policy Controls	Y	Y	Y	Y	Y	Y
Urban Arrest Controls	N	Y	Y	N	Y	Y
Crime Controls	N	N	Y	N	N	Y
Demo Controls	N	N	Y	N	N	Y
Urbanicity Control	N	N	Y	N	N	Y
Year Fixed Effects	Y	Y	Y	Y	Y	Y
State Fixed Effects	Y	Y	Y	Y	Y	Y
N	1640	1383	1383	1640	1383	1383

This table provides the results of difference-in-difference analyses estimating the effects of rejecting the third party doctrine on the total number of days of interception authorized per 100,000 people in a given state in a given year. A Poisson regression model was used, and robust standard errors were used to account for clustering at the state level. State and year fixed effects were included on all regressions. *** denotes statistical significance at the 0.01 level; ** denotes statistical significance at the 0.05 level; *** denotes statistical significances at the 0.1 level.

Table D.2A. Effect of Rejecting the Third Party Doctrine on Number of Initial Intercept Requests, Omitting States that Never Address Third Party Doctrine

	(I)	(I)	(I)	(II)	(II)	(II)
Any Rejection of TPD	-0.476	-0.490	-0.198			
	(0.296)	(0.326)	(0.179)			
Rejection of TPD for Phone Records				-0.360	-0.480	-0.263
				(0.254)	(0.301)	(0.209)
Rejection of TPD for Bank Records				-0.268	-0.362	0.103
				(0.237)	(0.277)	(0.138)
Rejection of TPD for Location Info				-0.057	-0.324	0.020
				(0.391)	(0.464)	(0.198)
Policy Controls	Y	Y	Y	Y	Y	Y
Urban Arrest Controls	N	Y	Y	N	Y	Y
Crime Controls	N	N	Y	N	N	Y
Demo Controls	N	N	Y	N	N	Y
Urbanicity Control	N	N	Y	N	N	Y
Year Fixed Effects	Y	Y	Y	Y	Y	Y
State Fixed Effects	Y	Y	Y	Y	Y	Y
N	820	672	672	820	672	672

This table provides the results of difference-in-difference analyses estimating the effects of rejecting the third party doctrine on the number of requests for communication intercepts made per 100,000 people in a given state in a given year. A Poisson regression model was used, and robust standard errors were used to account for clustering at the state level. State and year fixed effects were included on all regressions. *** denotes statistical significance at the 0.01 level; ** denotes statistical significance at the 0.05 level; *** denotes statistical significances at the 0.1 level.

Table D.2B. Effect of Rejecting the Third Party Doctrine on Overall Number of Wiretap Requests, Omitting States that Never Address Third Party Doctrine

	(III)	(III)	(III)	(IV)	(IV)	(IV)
Any Rejection of TPD	-0.478**	-0.447	-0.181			
	(0.240)	(0.276)	(0.153)			
Rejection of TPD for Phone Records				-0.632**	-0.718**	-0.451**
				(0.270)	(0.329)	(0.225)
Rejection of TPD for Bank Records				-0.282	-0.358	-0.057
				(0.217)	(0.252)	(0.147)
Rejection of TPD for Location Info				-0.009	-0.087	0.141
				(0.325)	(0.430)	(0.205)
Policy Controls	Y	Y	Y	Y	Y	Y
Urban Arrest Controls	N	Y	Y	N	Y	Y
Crime Controls	N	N	Y	N	N	Y
Demo Controls	N	N	Y	N	N	Y
Urbanicity Control	N	N	Y	N	N	Y
Year Fixed Effects	Y	Y	Y	Y	Y	Y
State Fixed Effects	Y	Y	Y	Y	Y	Y
N	820	672	672	820	672	672

This table provides the results of difference-in-difference analyses estimating the effects of rejecting the third party doctrine on the number of requests for communication intercepts made per 100,000 people in a given state in a given year. A Poisson regression model was used, and robust standard errors were used to account for clustering at the state level. State and year fixed effects were included on all regressions. *** denotes statistical significance at the 0.01 level; ** denotes statistical significance at the 0.05 level; *** denotes statistical significances at the 0.1 level.

Table D.2C. Effect of Rejecting the Third Party Doctrine on Total Days of Interception Authorized, Omitting States that Never Address Third Party Doctrine

	(V)	(V)	(V)	(VI)	(VI)	(VI)
Any Rejection of TPD	-0.586**	-0.566*	-0.215			
	(0.240)	(0.049)	(0.136)			
Rejection of TPD for Phone Records				-0.741***	-0.784***	-0.522***
				(0.234)	(0.301)	(0.197)
Rejection of TPD for Bank Records				-0.320	-0.463**	-0.049
				(0.217)	(0.229)	(0.131)
Rejection of TPD for Location Info				-0.141	-0.249	0.090
				(0.316)	(0.408)	(0.191)
Policy Controls	Y	Y	Y	Y	Y	Y
Urban Arrest Controls	N	Y	Y	N	Y	Y
Crime Controls	N	N	Y	N	N	Y
Demo Controls	N	N	Y	N	N	Y
Urbanicity Control	N	N	Y	N	N	Y
Year Fixed Effects	Y	Y	Y	Y	Y	Y
State Fixed Effects	Y	Y	Y	Y	Y	Y
N	820	672	672	820	672	672

This table provides the results of difference-in-difference analyses estimating the effects of rejecting the third party doctrine on the total number of days of interception authorized per 100,000 people in a given state in a given year. A Poisson regression model was used, and robust standard errors were used to account for clustering at the state level. State and year fixed effects were included on all regressions. *** denotes statistical significance at the 0.01 level; ** denotes statistical significance at the 0.05 level; *** denotes statistical significances at the 0.1 level.

Appendix E. References, Reconsidering Law Enforcement Use of Technological Search and Seizure

Case Law

Jacobellis v. Ohio, 378 U.S. 184 (1964).

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

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

Oliver v. United States, 466 U.S. 170 (1984).

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

United States v. Dunn, 480 U.S. 294 (1987).

Kyllo v. United States, 533 U.S. 27 (2000).

United States v. Jones, 565 U.S. 945 (2012).

Florida v. Jardines, 569 U.S. 1 (2013)

United States v. Graham, 2016 U.S. App. LEXIS 9797 (4th Cir. 2016).

Statutory Law and Constitutional Provisions

Col. Rev. Stat. sec. 16-3-303.5

Mont. Code Ann. Sec. 46-5-110.

U.S. Const. Amend. IV.

50 U.S.C. §1801(f)

H.R. 4887 (2016).

Articles

Adminstrative Office of the U.S. Courts (2015). "Wiretap Reports." http://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports

Balkovich, Edward, Don Prosnitz, Anne Bosutead, and Steven C. Isley (2015). "Electronic Surveillance of Mobile Device: Understanding the Mobile Ecosystem and Applicable Surveillance Law." RAND Report RR800.

Bankston, Kevin S, and Ashkan Soltani (2014). “Tiny Constables and the Cost of Surveillance: Making Cents Out of *United States v. Jones*.” *The Yale Law Journal* 123: 335.

Brennan, William J. (1977). "State Constitutions and the Protection of Individual Rights" 90 (3): 489-504.

Campbell, John L., Charles Quincy, Jordan Osserman, and Ove K. Pedersen (2013). "Coding In-depth Semistructured Interviews: Problems of Unitization and Intercoder Reliability and Agreement." *Sociological Methods & Research* 42(3): 294-320.

Copes, H., et al. (2011). "A content analysis of ethnographic research published in top criminology and criminal justice journals from 2000 to 2009." *Journal of Criminal Justice Education* 22(3): 341-359.

Dempsey, James X. (2012). "Keynote Address: The Path to ECPA Reform and the Implications of *United States v. Jones*." *University of Southern Florida Law Review* 47:225-244.

DiCicco□Bloom, B. and B. F. Crabtree (2006). "The qualitative research interview." *Medical education* 40(4): 314-321.

Farivar, Cyrus (2013). "Google stands up for Gmail users, requires cops to get warrant." *Ars Technica*, *available at* http://arstechnica.com/tech-policy/2013/01/google-stands-up-for-gmail-users-requires-cops-to-get-a-warrant/.

Frenkel, Monte (2013). "Can a Balance Between Privacy and Security Ever Be Struck?" Brennan Center for Justice, https://www.brennancenter.org/blog/can-balance-between-privacy-and-security-ever-be-struck.

Gallagher, Ryan (2013). "Meet the machines that steal your phone's data." *Ars Technica* Sept. 25, 2013, http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/.

Google (2016). *Transparency Report*. https://www.google.com/transparencyreport/

Grosche, Christian and Frank Steiner (1994). "How to Solve Path Integrals in Quantum Mechanics." *Journal of Mathematical Physics* 36.5 (1994): 2354-2385.

Henderson, Stephen E. (2006). “Learning From All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information From Unreasonable Search” Catholic University Law Review 55 (2): 373.

Hosein, Gus and Caroline Wilson Palow (2013). "Modern Safeguards for Modern Surveillance: An analysis of innovations in communications surveillance techniques." *Ohio State Law Journal* 74: 1071.

Julie, Richard S. (2000). "High-Tech Surveillance Tools and the Fourth Amendment: Reasonable Expectations of Privacy in the Technological Age." *American Criminal Law Review* 37:127-143.

Kerr, Orin S. (2004). "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution." Michigan Law Review 102(5): 801-888.

Kerr, Orin S. (2007). "Four Models of Fourth Amendment Protection." *Stanford Law Review* 60 (2): 503.

Kerr, Orin S. (2011). "An Equilibrium-Adjustment Theory of the Fourth Amendment." *Harvard Law Review* 125(2): 476-543.

Mayer, Jonathan, Patrick Mutchler, and John C. Mitchell (2016). "Evaluating the privacy properties of telephone metadata." Proceedings of the National Academy of Sciences 113 (20): 5536-6641.

Minzner, Max and Christopher M. Anderson (2013). "Do Warrants Matter?" *Review of Law & Economics* 9(2): 169-196.

Nunn, Samuel (2008). "Measuring criminal justice technology outputs: The case of Title III wiretap productivity, 1987-2005." *Journal of Criminal Justice* 36(4): 344-353.

Ohm, Paul K (2012). "The Fourth Amendment in a World Without Privacy." *Mississippi Law Journal* 81(5):1309-1356.

Owsley, Brian L. (2013). "The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in its Electronic Surveillance." *Journal of Constitutional Law* 16:1-48.

Pell, Stephanie K. and Christopher Soghoian (2014). "Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy." Harvard Journal of Law and Technology 28(1): 1-75.

Pierson, Paul (2000). "Increasing Returns, Path Dependence, and the Study of Politics." *American Political Science Review* 94(2): 251-267.

SEARCH.org (2016). "About Us." Accessed April 13. http://www.search.org/about-search/.

Selinger, Evan and Woodrow Hartzog (2014). "Obscurity and Privacy." in Routledge Companion to Philosophy of Technology, edited by Joseph Pit and Ashley Shewwi.

Solove, Daniel J. (2002). "Digital Dossiers and the Dissipation of Fourth Amendment Privacy." *Southern California Law Review* 75(5):1083-1168.

Spencer, Shaun B. (2013). "The Surveillance Society and the Third-Party Privacy Problem." *South Carolina Law Review* 65: 373-410.

Strange, Jeff (2015). “A Primer on Wiretaps, Pen Registers, and Trap and Trace Devices.” March 11.

Sturges, J. E. and K. J. Hanrahan (2004). "Comparing telephone and face-to-face qualitative interviewing: a research note." *Qualitative Research* 4(1): 107-118.

Surden, Harry (2007). “Structural Rights in Privacy.” *Southern Methodist University Law Review* 60: 1605.

Zetter, Kim (2015). “Turns Out Police Stringray Spy Tools Can Indeed Record Calls.” Wired, https://www.wired.com/2015/10/stingray-government-spy-tools-can-record-calls-new-documents-confirm/.

Appendix F. Full List of Considerations for Using Electronic Surveillance and Commercial Requests

Category	Electronic Surveillance	Commercial Requests
Legal Constraints	• Legal Barriers to Surveillance Use • Cost of Using Surveillance	• Legal Barriers to Surveillance Use • Cost of Using Surveillance
Resource Constraints	• Manpower Requirements • Available Resources • External Funding	• Manpower Requirements • Available Resources
Safety Concerns	• Officer Safety • Public Safety	• Officer Safety • Public Safety
Investigatory Concerns	• Facts of Case • No Alternative Surveillance • Type of Crime Committed • Use During Prosecution • Keep Informant Confidential • Next Form of Surveillance	• Type of Crime Committed • Use During Prosecution • Use During Investigation • Speed of Technique
Information Concerns	• Quality of Information • Type of Information Needed	• Quality of Information • Type of Information Needed • Resolution • Retention • Company in Possession of Information • Technical Difficulty of Obtaining Information