The Future of the Fourth Amendment: Guardian of the First Amendment

A THESIS
SUBMITTED TO THE FACULTY OF
UNIVERSITY OF MINNESOTA
BY

Alexander Vlisides

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF ARTS

Professor Jane Kirtley, Advisor

May 2015

© Alexander Vlisides 2015

ACKNOWLEDGEMENTS

Thank you very much to my committee: Professor Jane Kirtley, whose feedback over the last two years has made me into a writer capable of taking on this project; Professor JaneAnne Murray, for her expertise and positivity; and Professor Giovanna Dell‘Orto, for her interest and willingness to help.

To Tana, for her love, dreams, and endless support; and to my family, for teaching me to wrestle with big problems while living a life filled with small joys.

ABSTRACT

Modern technology records unprecedented amounts of data about individuals, and developments in surveillance technologies have removed many practical limitations on government collection of this information. A Fourth Amendment test called the third party doctrine permits the U.S. government to collect vast amounts of this electronically-stored data without any individualized suspicion. This thesis explores how the failure to create legal barriers preventing indiscriminate data collection chills citizens' First Amendment rights. Courts, legal scholars and social scientists have documented how pervasive surveillance restricts free expression and even free thought. This thesis endorses a technology-centered approach to the Fourth Amendment, which asks whether government's method of collection has the capacity to facilitate broad, indiscriminate surveillance. This approach better protects free expression and reasonable expectations of privacy by focusing directly on the fundamental challenge facing modern Fourth Amendment jurisprudence: the current practical and constitutional feasibility of mass surveillance methods that chill First Amendment rights.

TABLE OF CONTENTS

LIST OF FIGURES

> "When the framers wrote the Fourth Amendment about searches and seizures, they didn't envision wire taps. Therefore, the first decision was, 'Well, the Fourth Amendment doesn't apply to this.' But it became pretty clear pretty quickly that allowing people to intercept private conversations constituted the same sort of search and seizure of material that the framers want[ed] to protect. So you try to find, at least I do… what the fundamental principle underlying the constitutional protection is, and apply it to new issues and new technology. … I think that is going to be the real challenge for the next 50 years: How we do adapt old, established rules to new technology?"[1]

In the 2012 speech quoted above, U.S. Supreme Court Chief Justice John Roberts addressed the challenge at the core of modern Fourth Amendment[2] law: how do protections designed for old technologies apply to the technologies that replace them? This challenge is particularly acute when protecting against electronic searches and seizures, because in recent years, technology has changed the basic nature of how people communicate and store their information. Because of these changes, laws regarding searches and seizures now play a central role in protecting citizens' First Amendment rights. In creating Fourth Amendment law, courts must recognize this development and design standards which can adapt to new technologies while protecting First Amendment rights.

The core of American laws regarding the government's ability to search and seize is individuals' reasonable expectations of privacy. The Fourth Amendment restricts

[1] John Roberts, Chief Justice, United States Supreme Court, Centennial Lecture Series at Rice University (Oct. 17, 2012), *available at* https://mediacore.rice.edu/media/centennial-lecture-series-a-conversation-with-the-.

[2] U.S. Const. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

government action that invades an individual's expectation of privacy if that expectation is one society recognized as reasonable.[3] This standard separates investigative methods considered a Fourth Amendment "search" from those that do not trigger Fourth Amendment protections.[4] If a method does not constitute a search, government agents can perform this action without justification. If a method does constitute a search, the government may perform the search only if it acquires a search warrant or can justify the action under an exception to the warrant requirement.[5] The exclusionary rule means that if police invade a suspect's reasonable expectations of privacy without a warrant or applicable warrant exception, the evidence derived from this search will generally be inadmissible at trial.[6]

The Fourth Amendment is technology-neutral. Its protections exist not to prevent some particular form of invasion, but to guarantee the substantive right against unreasonable search and seizure.[7] This means that a Fourth Amendment standard should apply to new technology in a way that continues to reflect people's reasonable expectations of privacy. Such a standard should both protect established Fourth Amendment rights and preserve the ability of law enforcement to investigate crimes. Current Fourth Amendment doctrine often fails to serve these interests. In particular, a test known as the third party doctrine, which very often governs searches of electronic

[3] *Id.* at 361 (Harlan, J., concurring).
[4] *See* Orin Kerr, *Four Models of Fourth Amendment Protection*, STAN. L. REV. 503 (2007).
[5] Katz v. United States, 389 U.S. 347, 362 (1967) (Harlan, J., concurring).
[6] Davis v. United States, 131 S. Ct. 2419, 2423 (2011) ("[T]his Court created the exclusionary rule, a deterrent sanction that bars the prosecution from introducing evidence obtained by way of a Fourth Amendment violation.").
[7] *See Katz*, 389 U.S. at 359 ("Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.").

information, generally holds that individuals cannot have a reasonable expectation of privacy in information held by or shared with third parties. For instance, the Supreme Court has held that individuals have no reasonable expectation of privacy in the numbers dialed on a telephone, as callers are aware this information is disclosed to the phone company.[8] In his speech, Chief Justice Roberts was describing the goal of articulating a technology-neutral standard for solving novel Fourth Amendment problems. This will require revising and reconceptualizing Fourth Amendment law, including the third party doctrine.

Changes to this legal standard will have a great impact on the privacy of citizen communications and personal information. This standard will determine how Americans' electronic communications and information can be intercepted and surveilled by their government. The electronic information Justice Roberts referred to creates Fourth Amendment problems that implicate the First Amendment. Interpersonal communications, data revealing personal associations, and personal data electronically stored with a third party—akin to the Fourth Amendment's protected "papers"—all implicate strong First Amendment interests.

This thesis will address two central factors that courts must consider in creating a Fourth Amendment standard. First, Fourth Amendment law must apply in a technology-neutral manner. To uphold the guarantees of the Fourth Amendment, people must be free from unreasonable searches of their communications regardless of how they transmit or store information. Second, when addressing Fourth Amendment cases that involve

[8] Smith v. Maryland, 442 U.S. 735, 743 (1979).

technologies that can facilitate indiscriminate surveillance, courts must consider the chilling effect on lawful expression and conduct that this surveillance can impose.

This thesis will then expand upon work by other scholars and endorse a technology-centered approach. This approach suggests that courts could analyze modern surveillance technologies by asking whether those technologies can facilitate broad and indiscriminate surveillance that invades reasonable expectations of privacy. It focuses directly on the aspects of modern surveillance that are quantitatively and qualitatively different from traditional law enforcement methods and which threaten to impose significant chilling effects. This approach recognizes that while the methods available to law enforcement must change with technology, the allowable incursions into citizens' privacy should remain essentially the same. In other words, "the Fourth Amendment [should] permit access to that which technology hides," but also "should protect that which technology exposes."[9] The technology-centered approach accomplishes this by focusing reform on the modern collection methods capable of exposing previously private or practically obscure information on a mass scale, while preserving human investigation methods that do not pose a similar threat. It provides a technology-neutral Fourth Amendment path forward, which maintains fundamental protections from government intrusion and protects against mass chilling effects, while preserving law enforcement's ability to use traditional warrantless methods.

[9] Orin Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561, 580 (2009).

I. RESEARCH QUESTIONS

The goal of this thesis is to analyze the Fourth Amendment protections for electronic information, examine the First Amendment impacts of lawful U.S. surveillance, and propose a reformed theoretical framework for courts to apply to Fourth Amendment problems. This requires research on several elements of these issues. First:

RQ1: How do courts determine when government information collection constitutes a Fourth Amendment search of electronic information?

RQ1a: What is the theoretical justification for distinguishing collection that constitutes a search from collection that does not?

RQ1b: Do the tests applied by courts serve these theoretical justifications?

Challenging the current Fourth Amendment doctrine requires a detailed analysis of its foundations. This section will explore how these foundations led to the third party doctrine as a method of solving Fourth Amendment problems and why this was viewed as a useful and necessary theory. It then will examine how this doctrine has been applied and whether its application has successfully served its theoretical justifications.

RQ2: Are there First Amendment chilling effects created by the type of government surveillance current U.S. law permits?

RQ2a: What are the chilling effects associated with pervasive, non-politically targeted surveillance?

RQ2b: How have changes in technology created chilling effects associated with surveillance?

This research question focuses on how a legal doctrine incapable of recalibrating based on fundamental changes in the scope of surveillance can affect First Amendment rights. The goal is to focus specifically on the chilling effects caused by lawful U.S. government surveillance. This section aims to explore the ways in which modern technology has facilitated indiscriminate surveillance, and to integrate research on these changes with research on how surveillance chills First Amendment-protected activities. Only by scrutinizing the First Amendment concerns as carefully as, for instance, concerns about law enforcement overreach, can one make a Fourth Amendment reform proposal that genuinely balances these and other competing concerns.

Next, the thesis will seek to answer the question posed by the critique of current doctrine and the examination of chilling effects: what is a superior alternative? Particularly, it will focus on the obstacles to creating a technology-neutral paradigm that protects First Amendment interests to the greatest extent possible while accommodating other considerations such as law enforcement effectiveness. The thesis will examine other proposals for new approaches and their strengths and weaknesses. Finally it will endorse a revised approach to solving these problems.

RQ3: How can courts create a technology-neutral standard for determining whether a Fourth Amendment search has occurred that protects First Amendment rights?

RQ3a: What new or revised approaches have scholars proposed to determine when an electronic search has occurred?

RQ3b: What principles can create a technology-neutral Fourth Amendment approach that minimizes First Amendment chilling effects while empowering the government to investigate crimes?

II. FOURTH AMENDMENT JURISPRUDENCE AND THE TECHNOLOGY-NEUTRAL APPROACH

a. LITERATURE REVIEW

The third party doctrine is a legal test arising from this foundation that holds "that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[10] Under this doctrine, when the government collects information that was conveyed to a third party, it is generally not considered a Fourth Amendment search.[11] This information can be collected without any Fourth Amendment constraint. Thus the government can collect information that has been willingly exposed to the public[12] or information possessed by third parties such as communications companies[13] without a warrant.

[10] *Smith*, 442 U.S. at 743-44.
[11] RICHARD THOMPSON, CONG. RESEARCH SERV., THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE 1 (2014).
[12] *See, e.g.*, California v. Greenwood, 486 U.S. 35, 43-44 (1988).
[13] *See, e.g.*, *Smith*, 442 U.S. at 743-44.

The third party doctrine, particularly as applied to electronic searches, has been the subject of much debate among legal scholars. George Washington University Law School Professor Orin Kerr is a prominent academic defender of the third party doctrine.[14] His 2007 article *The Case for the Third Party Doctrine* made theoretical and pragmatic arguments in support of the doctrine.[15] Kerr argued that the doctrine is technology-neutral because it prevents criminals from exploiting technology to gain greater Fourth Amendment protections.[16] Also, Kerr argues, the doctrine provides a bright line rule needed on this issue to give law enforcement the operational clarity required for effective policing.[17] His defense of the doctrine also spurred a public debate with several other Fourth Amendment scholars. In a 2009 Symposium Issue of the *Berkeley Technology Law Journal*, Professors Richard Epstein and Erin Murphy critiqued *The Case for the Third Party Doctrine*, and Professor Kerr responded in support of the doctrine.[18]

However, the overwhelming majority of legal scholarship is critical of the doctrine. Critiques tend to focus on two major shortcomings. First, it does not reflect citizens' subjective expectations of privacy and is therefore not consistent with basic

[14] Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 44 (2011); Julian Sanchez, *The Talking Points for NSA's Dragnet Don't Hold Up*, CATO INSTITUTE (July 24, 2013), http://www.cato.org/blog/talking-points-nsas-dragnet-dont-hold.
[15] *The Case for the Third Party Doctrine*, *supra* note 9.
[16] *Id.* at 573.
[17] *Id.* at 581.
[18] Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199 (2009); Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr,* 24 BERKELEY TECH. L.J. 1239 (2009); Orin S. Kerr, *Defending the Third-Party Doctrine: A Response to Epstein and Murphy*, 24 BERKELEY TECH. L.J. 1229 (2009).

Fourth Amendment principles.[19] This first critique is supported by several different arguments. Many argue that the third party doctrine is based on the flawed premise that privacy is a binary concept that is waived when disclosed to another party.[20] In other words, it is unacceptable to "treat[] exposure to a limited audience as identical to exposure to the world."[21]Another argument is that because of changes in technology, the decision to reveal information to third parties is often not sufficiently voluntary to justify its use as a waiver of privacy rights over that information.[22] For instance, Vanderbilt University Law School Professor Christopher Slobogin argued that under the third party doctrine, it could be necessary for an individual to refuse educational or medical advances because they may expose personal information to third parties, an irrational and potentially harmful result.[23]

The second major critique is that the doctrine justifies an unacceptable level of government intrusion. As changes in technology expose much more of people's information to third parties, many scholars have made normative arguments that particular collection methods permitted by the third party doctrine are sufficiently intrusive to trigger Fourth Amendment protection. Some scholars focus on the problematic consequences of allowing particular collection methods such as cell phone

---

[19] *See, e.g.,* Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 643 (2013).
[20] *See, e.g.,* Susan Brenner & Leo Clarke, *Fourth Amendment for Shared Privacy Rights in Stored Transactional Data*, 14 J. L. & POL'Y 211, 258 (2006).
[21] Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122 (2002).
[22] *See, e.g.,* Mary Graw Leary, *Katz on A Hot Tin Roof-Saving the Fourth Amendment from Commercial Conditioning by Reviving Voluntariness in Disclosures to Third Parties*, 50 AM. CRIM. L. REV. 341, 343 (2013).
[23] CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 156 (2007).

location tracking[24] or communication over social media[25] to undermine the third party doctrine more generally. Others have argued that although the third party doctrine may be viable as applied to traditional collection methods, it must be interpreted differently with respect to Internet communication.[26]

However, critiques are much more common than solutions.[27] This thesis will closely examine several proposed paradigms intended to replace the third party doctrine, as these will demonstrate both the template for and difficulties of proposing such a solution. For instance, Mosaic Theory is the recent Fourth Amendment reform proposal that has gained the most traction with scholars[28] and courts.[29] The premise of Mosaic Theory is that information collected through means not considered a Fourth Amendment "search" nevertheless may constitute a search when large data sets are aggregated to create a revealing "mosaic" of a person's life.[30] David Gray & Danielle Citron's article *The Right to Quantitative Privacy* provides a proposal based on technology-centered approach.[31] This approach would determine whether the use of a surveillance technology constitutes a search by asking whether it has the capability to facilitate broad,

---

[24] Michael T.E. Kalis, *Ill Suited to the Digital Age: Fourth Amendment Exceptions and Cell Site Location Information Surveillance*, 13 U. PITT. J. TECH. L. POL'Y 1 (2013).
[25] Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1 (2013).
[26] Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1403 (2004).
[27] *See, e.g.*, Murphy, *supra* note 18, at 1251 ("So if I want some kind of constitutional third-party protection, and I recognize that it cannot simply be contiguous with the defendant's Fourth Amendment rights, then how might I imagine the doctrine? Truthfully, I have no idea.").
[28] *See, e.g,* Erin Smith Dennis, *A Mosaic Shield: Maynard, the Fourth Amendment, and Privacy Rights in the Digital Age*, 33 CARDOZO L. REV. 737, 738-44 (2011); Jace Gatewood, *District of Columbia Jones and the Mosaic Theory-in Search of A Public Right of Privacy: The Equilibrium Effect of the Mosaic Theory*, 92 NEB. L. REV. 504 (2014).
[29] *See infra* Part IV.a.
[30] United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) *aff'd* in part *sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).
[31] David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013).

indiscriminate surveillance.[32] Daniel Solove's *The First Amendment as Criminal Procedure* provides another perspective, seeking to expand protections against subpoenas based on the information's First Amendment value, rather than expanding the warrant requirement under the Fourth Amendment as many other scholars have proposed.[33]

b. ANALYSIS

This section will analyze the development of Fourth Amendment jurisprudence, particularly the third party doctrine. It will demonstrate that although the doctrine arose from reasonable decisions given the contemporaneous technology and the facts at issue, it is a limited, technology-specific solution for Fourth Amendment problems. Specific attention will be paid to the logic of its application to new technologies. In some cases, the justifications for the third party doctrine are strong and serve the intended interests, but in other cases, they fail to serve these interests. This section will also demonstrate the crucial weaknesses of the third party doctrine, which have led to several recent decisions which rejected the third party doctrine as applied to the facts of the case. The third party doctrine creates problematic results by basing analysis on technological details of communication rather than the consequences of an unreasonable search. In these cases and as applied to emerging technologies, the third party doctrine fails as a technology-neutral solution to Fourth Amendment problems.

[32] *Id.* at 69.
[33] Daniel Solove, *The First Amendment As Criminal Procedure*, 82 N.Y.U. L. REV. 112 (2007).

One of the cases often cited as categorically establishing the third party doctrine is *Smith v. Maryland*.[34] In *Smith*, a man was suspected of robbing a woman's home and placing harassing phone calls to her. The Supreme Court ruled that law enforcement use of a pen register, which tracks the numbers dialed from the suspect's phone, did not constitute a Fourth Amendment search of the caller's home.[35] The Court ruled that because the suspect should have been aware that the third party telephone company recorded his dialed calls, he could have no reasonable expectation of privacy in that information.[36]

In *Smith* and many other cases following the doctrine, no Fourth Amendment search took place and the court correctly upheld the warrantless collection. The result was justified, but the reasoning—that based on an analogy to a pen register, there is no expectation of privacy in any information shared with a third party—is deeply flawed. The outcome in *Smith* was correct. But the reasoning of the third party doctrine is inconsistent with the Fourth Amendment, and that has been steadily revealed by the progression of technology. The categorical rule from *Smith* creates aberrant and unreasonable results when applied to collection using different technology. The third party doctrine has been the target of scholarly criticism almost since its inception.[37] But, as explored above, scholars and courts have struggled to create a viable alternative.[38]

---

[34] THOMPSON, *supra* note 11.
[35] Smith v. Maryland, 442 U.S. 735 (1979).
[36] *Id.* at 743.
[37] *See The Case for the Third Party Doctrine*, *supra* note 9, at 563, fn. 5 (2009) ("A list of every article or book that has criticized the doctrine would make this the world's longest law review footnote."). *See, e.g.*, Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy*", 34 VAND. L. REV. 1289, 1315 (1981); Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-first Century*, 65 IND. L.J. 549, 564-66 (1990).
[38] *See, e.g.*, Murphy, *supra* note 18, at 1251.

With no clearly articulated alternative, courts have opted to adhere to the often arbitrary but definitive tool of the third party doctrine.

In addition to analyzing the progression of Fourth Amendment doctrine, this section explores an indispensable aspect of any Fourth Amendment solution: technology-neutrality. This concept has been explored by influential Fourth Amendment scholar Orin Kerr who stated, "*Katz* effectively required technological neutrality."[39] Under this approach, protection of information should not be based on arbitrary distinctions between technologies. As an example, the facts from *Smith* can illustrate this approach. Police should have access to a tool like a pen register because the telephone allows for previously public, and therefore observable, criminal action to be committed purely in private. Traditionally, one would have had to travel public streets to harass another person in her home, which means that the police would be able to observe that travel and potentially gather probable cause to obtain a search warrant. However, technology allowed the defendant to harass over the phone, rather than travelling to her home. In other words, a pen register allowed law enforcement to gather information analogous to what would have been accessible without a warrant before the telephone existed. To bar law enforcement from collecting such information would threaten to prevent police officers from collecting the type of information necessary to make a showing of probable cause to obtain of a warrant.[40] The Constitution is not a promise to handcuff law enforcement unnecessarily to ineffective methods.

[39] *The Case for the Third Party Doctrine*, *supra* note 9, at 580.
[40] This analogy is explored further in Professor Orin Kerr's analysis of *Smith*. *Id.* at 577-78.

This is an example of how Kerr argued that the third party doctrine is technology neutral.[41] A technology-neutral approach focuses on the substitution effect of technology.[42] Although the mechanism of new methods of communication or information storage may be completely novel, their function often resembles the technology of the past. This approach recognizes that while the methods available to law enforcement must change with technology, the allowable incursions into citizens' privacy should stay essentially the same. In other words, "the Fourth Amendment [should] permit access to that which technology hides," but also "should protect that which technology exposes."[43] The third party doctrine is an arbitrary and misguided tool to navigate this distinction.

Part one of this section will introduce the foundations of Fourth Amendment law as applied to communications and explore how past courts have attempted to create technology-neutral tests. Part two will provide an overview of the development of the third party doctrine, summarizing the reasoning of these precedents to demonstrate how the Court arrived at the categorical declaration in *Smith* that information shared with a third party was outside Fourth Amendment protection. Part three will examine the reasoning of recent cases that have questioned the viability of the third party doctrine. As lower courts and the Supreme Court reconsider this bright line approach to the Fourth Amendment, and privacy decisions in other contexts challenge some of the doctrine's underlying assumptions, is the third party doctrine a sufficient and coherent constitutional safeguard?

---

[41] *Id.* at 580.
[42] For more on "substitution effects," *see id.* at 577. *But see* Blake Ellis Reid, *Substitution Effects: A Problematic Justification for the Third-Party Doctrine of the Fourth Amendment*, 8 J. TELECOMM. & HIGH TECH. L. 613, 614 (2010).
[43] *The Case for the Third Party Doctrine*, *supra* note 9, at 580.

i. Foundations of the Fourth Amendment

In Anglo-American law, the rights of free expression and freedom from government searches are inextricably linked. In 18th century England, the push for rights against arbitrary government searches began in response to the press licensing system and the conferment of immense authority to those enforcing it.[44] The first cases rejecting the King's right to search a home without justification concerned searches of publishers.[45] In the foundational case *Entick v. Carrington and Three Other King's Messengers*, the court rejected the validity of a general warrant targeting a publisher of a political pamphlet and framed the protection from government search as necessary to protect speech.[46] Lord Camden wrote that if the warrantless searches were upheld, "the secret cabinets and bureaus of every subject in this kingdom will be thrown open to the search and inspection of a messenger, whenever the secretary of state shall think fit to charge, or even to suspect, a person to be the author, printer, or publisher of a seditious libel."[47]

In the American colonies, many residents agitated against a particular type of general warrant: the writ of assistance.[48] These writs empowered representatives of the Crown to conduct broad warrantless searches at their discretion, and a writ was valid for the lifespan of the King.[49] After the revolutionary war, the framers of the Bill of Rights

---

[44] F. SIEBERT, FREEDOM OF THE PRESS IN ENGLAND: 1476-1776, 173-76 (1952).
[45] M. Blane Michael, *Reading the Fourth Amendment: Guidance from the Mischief That Gave It Birth*, 85 N.Y.U. L. REV. 905, 910-11 (2010).
[46] 19 HOW. ST. TRI. 1029 (1765).
[47] *Id.*
[48] Michael, *supra* note 45, at 911.
[49] *Id.* at 908.

sought to restrict government power and the Fourth Amendment was designed to "ban general warrants and writs of assistance."[50]

Fourth Amendment jurisprudence has always been informed by this history. After the Fourth Amendment "remained for almost a century a largely unexplored territory,"[51] the Supreme Court confronted a warrantless search of personal papers in 1886 case *U.S. v. Boyd*. The Court recounted the history leading to the Fourth Amendment, including the protests against writs of assistance and the press rights at issue in *Entick*.[52] It then expounded upon the values of the Fourth Amendment, derived from this history. "It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense," Justice Bradly wrote. Rather the Fourth Amendment created a broader right against "the invasion of his indefeasible right of personal security, personal liberty and private property."[53] Bradley concluded, "[I]t is the invasion of this sacred right which underlies and constitutes the essence of Lord Camden's judgment [in *Entick*]."[54] The *Boyd* Court relied on the history of arbitrary searches used to target dissidents to explicate the values of personal privacy and liberty the Fourth Amendment protected.

In 1928, the Supreme Court decided *Olmstead v. United States*, its first major case confronting electronic surveillance. *Olmstead* is the "first decision" on the constitutionality of warrantless wiretaps that Chief Justice Roberts referred to in his speech and a foundational Fourth Amendment case. In this case, a criminal defendant whose telephone communications were recorded by law enforcement argued that this

[50] *Id.* at 912.
[51] JACOB LANDYNSKI, SEARCH AND SEIZURE AND THE SUPREME COURT 49 (1966).
[52] Boyd v. United States, 116 U.S. 616, 625-26 (1886).
[53] *Id.* at 630.
[54] *Id.*

evidence should be suppressed because the collection violated his Fourth Amendment rights.[55] A majority of the Supreme Court rejected this argument because the collection occurred through the tapping of telephone lines located outside of the defendant's property.[56] The government had not trespassed on the defendant's property in performing the relatively new method of collecting electronic, rather than physical, information. The Court held that for the Fourth Amendment to apply, the government must commit a physical intrusion into a constitutionally protected space.[57] Thus, the Court rejected the argument that a warrantless wiretap violated the Fourth Amendment.[58] Justice Brandeis challenged this property-based approach in his dissent, arguing that it adopted a dangerously narrow understanding of Fourth Amendment Protection.[59]

In particular, Brandeis warned of interpreting constitutional protections, such as those enumerated in the Fourth Amendment, in a way that limits their applicability to the problems of the past.[60] He reckoned back to the nation's founding to underscore the gravity of the threat, writing, "As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire-tapping."[61] He argued that when constitutional protections are formulated based only on traditional threats to liberty, courts sacrifice meaningful protection in the name of

[55] Olmstead v. United States, 277 U.S. 438, 456 (1928).
[56] *Id.* at 457 ("The insertions were made without trespass upon any property of the defendants. They were made in the basement of the large office building. The taps from house lines were made in the streets near the houses.").
[57] *Id.* at 466.
[58] *Id.*
[59] *Id.* at 472 (Brandeis, J., dissenting).
[60] *Id.* (Brandeis, J., dissenting) ("Legislation, both statutory and constitutional, is enacted, it is true, from an experience of evils, but its general language should not, therefore, be necessarily confined to the form that evil had theretofore taken.") (quoting Weems v. United States, 217 U.S. 349, 371 (1910)).
[61] *Id.* at 476 (Brandeis, J., dissenting).

decisional clarity.[62] Brandeis wrote that the constitution's protections must apply not only to "what has been but [to] what may be. Under any other rule a Constitution would indeed be as easy [to apply] as it would be deficient in efficacy and power."[63] Instead, Brandeis argued, the Court had no option but to do the difficult work of applying past principles to new problems, because without this forward-looking philosophy, "rights declared in words might be lost in reality."[64]

In *Olmstead*, this meant applying a theory of the Fourth Amendment that accounted for new technology. Brandeis concluded that any such theory must be defined by the effect of the intrusion, not its form.[65] Brandeis cited *Ex Parte Jackson*, an 1878 case in which the Court ruled that the government needed a warrant to open and examine the contents of a sealed envelope in the mail.[66] In *Jackson*, the Court reasoned that because the government could not search letters carried by individuals without a warrant, it would be unjust to allow the warrantless search of sealed letters in the mail, simply because they were entrusted to the postal service, an arm of the government.[67] Because of the parallel function of the postal service and the personal courier, sealed letters handled by either service were subject to the same warrant requirement.[68] Thus, law enforcement could inspect the outside of an envelope with impunity, but inspecting its contents

---

[62] *Id.* (Brandeis, J., dissenting). ("Clauses guaranteeing to the individual protection against specific abuses of power, must have a [] capacity of adaptation to a changing world.")
[63] *Id.* at 473 (Brandeis, J., dissenting).
[64] *Id.* (Brandeis, J., dissenting).
[65] *Id.* (Brandeis, J., dissenting).
[66] *Id.* at 475 (Brandeis, J., dissenting).
[67] Ex parte Jackson, 96 U.S. 727, 733 (1878) ("The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household.").
[68] *Id.*

required a warrant.[69] Comparing the wire taps at issue in *Olmstead* with the interception of the contents of mail, Brandeis explored the implications of a technology-neutral approach.[70] Of telephone conversations and mail, he wrote, "True, the one is visible, the other invisible; the one is tangible, the other intangible; the one is sealed, and the other unsealed; but these are distinctions without a difference."[71] The many technical distinctions that could be drawn between the two technologies were irrelevant in the face of one commonality: each facilitated private personal conversations between individuals. Brandeis' reasoning demanded a technology-neutral approach to the Fourth Amendment focused on the technology at issue and the effect of the invasion, not the practical method of a government invasion.

Brandeis's approach was echoed by a majority of the Supreme Court almost four decades later. Between 1928 and 1967, the number of U.S. households with a telephone more than doubled, from less than 40% to almost 90%, and the Supreme Court's jurisprudence regarding this technology evolved.[72] In *Berger v. New York*, the Court held that a wiretap on a private phone constituted an intrusion into a constitutionally protected area, deciding on the basis of the *Olmstead* majority's protected area doctrine that the physical intrusion necessary for the wiretap violated the Fourth Amendment.[73] Later that year in *Katz v. United States*, it overruled the protected area theory of the Fourth Amendment, finding that Fourth Amendment protection applied even to a conversation in

[69] *Id.*
[70] *Olmstead*, 277 U.S. at 475-76 (Brandeis, J., dissenting).
[71] *Id.* at 475 (Brandeis, J., dissenting).
[72] Michael DeGusta, *Are Smart Phones Spreading Faster than Any Technology in Human History?*, M.I.T. TECH. REV. (May 9, 2012), *http://www.technologyreview.com/news/427787/are-smart-phones-spreading-faster-than-any-technology-in-human-history/.*
[73] Berger v. New York., 388 U.S. 41, 44 (1967).

a public phone booth.[74] The "Fourth Amendment protects people, not places," the Court found.[75] It emphasized that Fourth Amendment protection did not hinge on whether a phone booth was a "constitutionally protected area" or minute details like whether a government-employed lip reader could have observed the defendant's statements.[76] Defendant Katz's constitutional rights were violated because the government obtained his communications, in which he had a reasonable expectation of privacy, without a warrant.[77] After *Katz*, to determine whether a Fourth Amendment search had occurred, courts were now to ask, first, if the individual had an expectation of privacy and second, if that expectation was one society recognized as reasonable.[78] Under this test, Katz could reasonably expect his telephone conversation in a public phone booth to be private.[79]

As Brandeis had in *Olmstead*, the Court emphasized the function of the communication, rather than the medium through which it occurred. "To read the Constitution," as allowing warrantless collection of a telephone call merely because it occurred on a public space "is to ignore the vital role that the public telephone has come to play in private communication."[80] The Court did not dispute that the conversation occurred in a portion of the public space, but allowing warrantless interception would not comport with the historically protected nature of private conversation.[81] The Court found that Katz could reasonably "assume that the words he utters into the mouthpiece will not

---

[74] Katz v. United States, 389 U.S. 347, 350 (1967) ("In the first place the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase constitutionally protected area.") (citations and internal quotation marks omitted).
[75] *Id.* at 351.
[76] *Id.* at 352-53.
[77] *Id.* at 359.
[78] *Id.* at 361 (Harlan, J., concurring).
[79] *Id.* at 359.
[80] *Id.* at 352.
[81] *Id.*

be broadcast to the world."[82] The Court explicitly held that the decision overruled "*Olmstead v. United States* which essentially rested on the ground that conversations were not subject to the protection of the Fourth Amendment."[83]

In *Katz*, the Court reconceptualized its approach to what constitutes a Fourth Amendment "search." Changes in technology had made a previously valid approach incapable of serving the role for which the Fourth Amendment was created. The Court recognized that the potential for electronic surveillance made the trespass-based approach insufficient to preserve the rights of citizens to exclude the state from his or her private affairs. It instead designed a technology-neutral standard based on reasonable expectations of privacy.

ii. Development of the Third Party Doctrine

The third party doctrine has its roots in undercover agent cases beginning in the 1950s.[84] In *Lee v. United States*, an undercover informant wore a hidden microphone to record the defendant's statements without his knowledge.[85] The Court recognized that Lee had chosen to speak confidentially with someone he trusted but had therefore opened himself to the possibility that that person would betray his trust.[86] Therefore Fourth Amendment protection did not attach.[87] In *Hoffa v. United States*, the Court affirmed the *Lee* Court's holding that the Fourth Amendment need not protect "a wrongdoer's

[82] *Id.*
[83] *Id.* at 362, fn. 23 (citation omitted).
[84] *See The Case for the Third Party Doctrine*, *supra* note 9, at 567.
[85] Lee v. United States, 343 U.S. 747, 749 (1952).
[86] *Id.* at 753.
[87] *Id.*

misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."[88]

These decisions were made before *Katz* fundamentally shifted the focus on Fourth Amendment doctrine to expectations of privacy. However, after *Katz*, the Supreme Court affirmed the admissibility of conversations secretly recorded by one of the parties based on a speaker's assumption of risk. In *United States v. White*, the majority found that society could not recognize a criminal's expectation that her companion would keep a conversation private as a reasonable one.[89] Under the Fourth Amendment, a person who has a private conversation assumes the risk that her partner chooses to lawfully record it for law enforcement use.[90] This line of cases stands for the proposition that when a conversation between two people is recorded by one of them, it is generally not a "search" under the Fourth Amendment. This is an important precedent that helped courts create the third party doctrine, which many courts have justified through an assumption of risk approach similar to these undercover agent cases.[91]

A few years later, when the Supreme Court confronted cases concerning the government collection of business records, it based its analysis on the undercover agent cases.[92] In these cases, the Court reasoned that for the purposes of the Fourth Amendment, transferring business records to a third party represented an assumption of risk similar to having a private conversation. Therefore government interception of these

[88] Hoffa v. United States, 385 U.S. 293, 302 (1966).
[89] White v. United States, 401 U.S. 745, 752 (1971).
[90] *Id.*
[91] Thompson, *supra* note 3411, at 8-9.
[92] *Id.*

records would not constitute a "search" under to the Fourth Amendment.[93] In *U.S. v. Miller*, the Court held that just as in a conversation, a bank depositor "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[94] In addition, the Court noted that the records did not document private matters, but rather financial records shared in the ordinary course of business. Thus the Fourth Amendment did not restrict the warrantless acquisition of such business records.

Next, the Court addressed the constitutional status of telephone metadata in *Smith v. Maryland*.[95] Police suspected that Smith had robbed a woman and was making harassing phone calls to her home.[96] The police asked the phone company to install a pen register on Smith's phone line, without a warrant.[97] The first day that the pen register was installed, it documented data on a call from Smith's phone to the female victim's phone, and the police used this information to obtain a search warrant and eventually arrest Smith.[98] The Supreme Court framed the issue as whether Smith "had a 'legitimate expectation of privacy' regarding the numbers dialed on his phone."[99] Based on several factors, such as that the numbers dialed are reproduced on a customer's monthly bill, the Court found that a reasonable consumer would be aware that the companies record that data.[100] And based on its previous third party doctrine holdings, the Court found that this awareness meant that a suspect could have no reasonable expectation of privacy in the

[93] *See, e.g.*, United States v. Miller, 425 U.S. 435, 443 (1976).
[94] *Id.*
[95] Smith v. Maryland, 442 U.S. 735 (1979).
[96] *Id.* at 737.
[97] *Id.*
[98] *Id.*
[99] *Id.* at 742.
[100] *Id.* at 742-43.

numbers he dialed.[101] By "expos[ing]" that information to the phone company, Smith "assumed the risk that the company would reveal to police the numbers he dialed."[102]

In *Smith*, the Court made the sweeping claim that "[t]his Court consistently has held that a person has no legitimate expectation of privacy in the information he voluntarily turns over to third parties."[103] But the Court's efforts to tie this finding to the analogy of sharing one's information with a person reveal some consideration of the function of the communication. The majority held that "[t]he switching equipment that processed those numbers [was] merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber."[104] Just as the recording devices in the undercover agent cases were merely a more reliable way of recording evidence than having the agent recount the conversation to authorities, the pen register was a stand-in for information that previously would have been revealed to a human operator.[105] Because it was already established that it did not constitute a Fourth Amendment search when one party to a conversation recorded it, by analogy, there was no such right over the information communicated in a "conversation" with a pen register. The Court concluded that it would be inconsistent with precedent "to hold that a different

[101] *Id.* at 744.
[102] *Id.*
[103] *Id.* at 743-44.
[104] *Id.* at 744.
[105] *Id.* at 744-45 ("The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber. Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.").

constitutional result is required because the telephone company has decided to automate."[106]

iii. Modern Courts Challenge the Third Party Doctrine

In *Klayman v. Obama*, U.S. District Court Judge Richard Leon, of the District of Washington, D.C., explicitly rejected the third party doctrine as articulated in *Smith*.[107] At issue in *Klayman* was the National Security Agency's (NSA) telephone metadata collection program, through which the U.S. government warrantlessly collected millions of Americans' call record information in bulk from telephone companies.[108] In June 2013, former NSA contractor Edward Snowden leaked classified documents revealing a variety of secret surveillance programs, including the telephone metadata collection program.[109] The leaks triggered worldwide debate about the scope of U.S. government surveillance, and provided the foundation for several legal challenges, including the *Klayman* case.[110]

Ruling on a preliminary injunction regarding the metadata collection program, Judge Leon found that "present-day circumstances—the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies" had so significantly changed from the past that *Smith* did not

---

[106] *Id.* at 745.
[107] *See* Klayman v. Obama, 957 F. Supp. 2d 1, 37 (D.D.C. 2013).
[108] *Id.* at 7.
[109] *Id.* at 10-11. *See generally* LUKE HARDING, THE SNOWDEN FILES (2014).
[110] *See* Alex Vlisides, *Snowden Leaks Continue to Reveal NSA Surveillance Programs, Drive U.S. and International Protests and Reforms,* SILHA BULLETIN (Dec. 2013), http://www.silha.umn.edu/news/Fall2013/SILHACENTERSnowdencoverstoryUniversityofMinnesota.html .

control.[111] The decision found a high likelihood that this collection program violated the plaintiff's Fourth Amendment rights and thus granted the preliminary injunction.[112] Leon ruled that although *Smith* held that a citizen does not have a reasonable expectation of privacy in her telephone metadata as to a limited, short-term search, the NSA's continuous and indiscriminate collection of all telephone metadata constituted a qualitatively different Fourth Amendment issue.[113] Judge Leon also found that modern cell phone usage meant that telephone metadata "'reflects a wealth of detail about … familial, political, professional, religious and sexual associations' … that could not have been gleaned from a data collection in 1979."[114] Thus, the suspicionless metadata collection was the type of intrusion the Fourth Amendment was meant to guard against and therefore the metadata program violated citizens' reasonable expectation of privacy.[115]

Leon's decision was highly controversial.[116] Beyond its intelligence and law enforcement ramifications, some questioned a District Court Judge's decision to reject what many considered a straightforward application of Supreme Court precedent from *Smith*.[117] But regardless of whether Leon showed appropriate judicial deference, the decision built upon a growing body of cases that grappled with, and questioned the

---

[111] *Klayman*, 957 F. Supp. 2d at 31.
[112] *Id.* at 9-10.
[113] *Id.* at 33.
[114] *Id.* at 36.
[115] *Id.* at 37.
[116] *See, e.g.,* Ashby Jones, *NSA Judge Is No Stranger To Controversial Rulings*, WALL ST. J. (Dec. 17, 2013), http://online.wsj.com/news/articles/SB10001424052702304403804579264413734088306.
[117] Andrew Cohen, *Is the NSA's Spying Constitutional? It Depends on Which Judge You Ask*, THE ATLANTIC (Dec. 27, 2013), http://www.theatlantic.com/national/archive/2013/12/is-the-nsas-spying-constitutional-it-depends-which-judge-you-ask/282672/ ("But Judge Leon ruled that the surveillance program *does* likely violate the Fourth Amendment's protection against unreasonable searches, and he rejected the *Smith* case as technologically outdated. One judge went around the precedent of *Smith*. The other judge embraced that precedent and said he had no right to ignore *Smith*.").

validity of, the growing privacy implications of applying the third party doctrine to many new technologies. In recent cases, U.S. Circuit Courts of Appeals have declined to extend the doctrine to new circumstances and the Supreme Court has challenged the viability of the doctrine as applied to new technology. Using Judge Leon's firm repudiation of the doctrine as a starting point, this section will examine the evolution of judicial challenges to the third party doctrine.

1. *United States v. Jones*

In 2013, the Supreme Court unanimously ruled that the government violated the Fourth Amendment when it installed a small GPS tracking device on a suspect's car and tracked his location for more than four weeks.[118] The five Justice majority in *Jones* concluded that because the government had physically invaded a constitutionally-protected space (the suspect's car), the warrantless search violated the Fourth Amendment. It did not reach the separate—and arguably more important—question of whether the GPS tracking violated the suspect's reasonable expectation of privacy.[119] Nevertheless, separate concurring opinions joined by five Justices rejected the core of the third party doctrine.

The facts of *Jones* do not precisely implicate the third party doctrine, but rather a closely related principle that "What a person knowingly exposes to the public … is not a subject of Fourth Amendment protection."[120] However these doctrines are interrelated and operate on many of the same assumptions, and in the context of GPS data, which

[118] United States v. Jones, 132 S. Ct. 945 (2012).
[119] *Id.* at 954.
[120] Katz v. United States, 389 U.S. 347, 351 (1967).

could be recorded by an attached device as in *Jones* or acquired from car or phone companies already collecting it, the doctrines may very well overlap. Moreover, the same technological developments that the concurring Justices confronted in *Jones* are those that challenge the third party doctrine, such as the development of technology recording and organizing massive amounts of data not previously thought to be protected by the Fourth Amendment. And finally, Justice Sotomayor's statement in *Jones* that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," reveals the degree to which the Justices understood that their discussion was equally applicable whether the government justified the warrantless collection of data under the public observation doctrine or the third party doctrine.[121] In fact, much third party doctrine scholarship actually treats the facts of *Jones* as being directly on-point.[122]

Although Justice Sotomayor joined the majority opinion, her separate concurring opinion argued that in a future case, the Court would need to overturn the third party doctrine.[123] Sotomayor agreed with Justice Alito's concurrence that long term GPS tracking triggers Fourth Amendment protection.[124] Her opinion also discussed how changes in technology have created the potential for large scale tracking of other types of information, such as Internet activity, purchases and telephone metadata, over which people often have a subjective expectation of privacy.[125] She wrote that for society to

[121] *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).
[122] *See, e.g.*, Dennis, *supra* note 28, at 738-44 (discussing the implications of *Maynard*).
[123] *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).
[124] *Id.* (Sotomayor, J., concurring).
[125] *Id.* (Sotomayor, J., concurring).

recognize these expectations as reasonable, the third party doctrine must be overturned.[126] Sotomayor found, "[W]hatever the societal expectations, [sensitive information shared with third parties] can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." [127]

These statements reject the third party doctrine as a decisive factor in Fourth Amendment analysis. Disclosure of information to third parties is, of course, relevant to one's expectation of privacy in it. But the third party doctrine commands precisely what Sotomayor rejects: that mere disclosure of information to third parties strips it of Fourth Amendment protection *for that reason alone.* Sotomayor's individual concurrence was the most explicit rejection of the third party doctrine, but her reasoning and inevitable conclusion were mirrored by the four other concurring Justices.

Justice Alito's concurrence, joined by three other Justices, challenged assumptions intrinsic to the third party doctrine. Alito stated that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[128] The fact that each data point of Jones' location on public streets was revealed voluntarily to the public contemporaneously does not mean that he had no reasonable expectation of privacy in four weeks of location data.[129] The concurrence declined to "identify with precision the point at which the tracking of this vehicle became a search,

[126] *Id.* (Sotomayor, J., concurring).
[127] *Id.* (Sotomayor, J., concurring).
[128] *Id.* at 964 (Alito, J., concurring).
[129] *Id.* (Alito, J., concurring).

for the line was surely crossed before the 4-week mark."[130] In other words, Alito rejects the premise that a citizen cannot have a reasonable expectation of privacy in a collection of publicly available data, where the individual has no reasonable expectation of privacy in any individual data point. This notion of privacy is a repudiation of the third party doctrine, at least its full application: that individuals cannot have a reasonable expectation of privacy in any information disclosed to third parties.

For Alito, recent technological changes have Fourth Amendment significance. In the past, "the greatest protections of privacy were neither constitutional nor statutory, but practical." GPS devices make the type of long-term location surveillance performed in *Jones* "relatively easy and cheap."[131] However until the quite recent past, such tracking would have been "difficult and costly and therefore rarely undertaken."[132] Now that technology has eliminated many of the practical bars to invasions of privacy, Alito concluded that the Fourth Amendment must play a different role in restricting the government.

This reasoning is reflective of the technology-neutral approach applied by Brandeis' dissent in *Olmstead* and by the majority in *Katz*. Rather than looking at the form of surveillance and analogizing it to a similar form from the past, Alito's concurrence looked at the effect of the surveillance and attempted to analogize it to a practice with a similar effect from the past. As an example, the GPS location data in *Jones* is quite similar to the information that a police officer could gather by observing a car on a public street. But Brandeis and the *Katz* majority understood that although a

[130] *Id.* (Alito, J., concurring).
[131] *Id.* (Alito, J., concurring).
[132] *Id.* at 963 (Alito, J., concurring).

wiretap's form of intrusion was most analogous to mere observation without invading a suspect's home, the effect of a wiretap was most analogous to the very types of searches through "papers and effects"[133] that the Fourth Amendment was intended to prevent. In *Jones*, the Alito concurrence recognized a similar historical inflection point, a time when the Court had to reconcile the divergence of two strands of a doctrine. Analogy to form pointed in one direction. Analogy to effect pointed in the other. In keeping with the foundational Fourth Amendment precedents, Alito put aside the formalistic commands of the third party doctrine and focused on the effect of the surveillance, which, in his view, amounted to a Fourth Amendment search. Although Alito declined to establish a clear Fourth Amendment rule in this case, he concluded that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[134]

Five Supreme Court Justices advocated in *Jones* for an understanding of the Fourth Amendment that would require a warrant for the collection of some types of information voluntarily shared with the public. This principle is inconsistent with the third party doctrine. And the four majority Justices who did not sign onto one of those opinions did not reject this premise, but rather did not reach the question. To argue that the Court is questioning the doctrine would understate the opinions expressed in *Jones*. Regardless of the degree to which future opinions may weigh disclosure to a third party as grounds for finding no reasonable expectation of privacy, the idea that "a person has

[133] U.S. CONST. amend. IV.
[134] *Jones*, at 964 (Alito, J., concurring).

no legitimate expectation of privacy in information he voluntarily turns over to third parties"[135] cannot be squared with the ideas expressed by five Justices in *Jones*.

2. Mosaic Theory and Replacement Effects

The concurrences in *Jones* focused on a particular weakness in the third party doctrine. The Justices questioned the premise that exposing one data point to the public means that there can be no privacy interest when the government collects a large amount of that data in a novel way. The idea that a collection of non-private information can implicate privacy interests is well represented in Supreme Court precedent, and some lower courts have found it controlling in the Fourth Amendment context. Within these cases, the reasoning reveals a decision by courts to reason based on the effect of the information rather than the technical details of how it was collected.

The Supreme Court has recognized that a person maintains a significant privacy interest even in information that has been voluntarily revealed by third parties. *U.S. Dept. of Justice v. Reporters Committee for Freedom of the Press* concerned the release of FBI rap sheets through Freedom of Information Act (FOIA) requests.[136] The rap sheets consisted of a computerized aggregation of publicly available arrest information about an individual.[137] In finding that individuals had a privacy interest in the rap sheets, the Court stated, "In an organized society, there are few facts that are not at one time or another divulged to another."[138] The Court rejected a "cramped notion of personal privacy" that

[135] Smith v. Maryland, 442 U.S. 735, 743-44 (1979).
[136] United States Dept. of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989).
[137] *Id.* at 752.
[138] *Id.* at 763.

would deny a right to privacy in a large collection of personal information on the grounds the each element of it was already publicly available.[139] "Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the county and a computerized summary located in a single clearinghouse of information."[140] The Court recognized that the "practical obscurity" of information could, in some cases, support a reasonable belief that the information was private.

Although the Court was interpreting FOIA, and therefore the decision is not controlling in Fourth Amendment decisions, its reasoning does challenge the basic assumptions of the third party doctrine. The Supreme Court rejected the premise that public availability of information vitiated any expectation of privacy in *Reporters Committee*. Its factual basis for doing so is no less valid in the Fourth Amendment context. Even in 1989, the Court found, "Hardly anyone in our society can keep altogether secret very many facts about himself. Almost every such fact, however personal or sensitive is known to someone else. Meaningful discussion of privacy, therefore, requires the recognition that ordinarily we deal not with an interest in total nondisclosure but with an interest in selective disclosure."[141] Although *Reporters Committee* did not raise a Fourth Amendment issue, it demonstrates that the Court has recognized a common sense distinction between a set of disparate and unconnected information and a cohesive and easily accessible compilation of that same information.

---

[139] *Id.* at 762-63.
[140] *Id.* at 764.
[141] *Id.* at 764 (quoting Kenneth Karst, *The Files*: *Legal Controls Over the Accuracy and Accessibility of Stored Personal Data*, 31 LAW & CONTEMP. PROB. 342, 343-44 (1966)).

The ideas explored in *Reporters Committee*, particularly the idea that "practical obscurity" of information can in some instances create a reasonable belief that the information in private, have been applied by other courts in the Fourth Amendment context, under the title "Mosaic Theory." Mosaic Theory generally refers to the idea that "even apparently innocuous information could be harmful if pieced together by a knowledgeable observer."[142] This term has been used in many contexts, including by the federal government to justify non-disclosure of unclassified documents requested under FOIA, on the theory that when combined and analyzed, they could threaten national security.[143] In Fourth Amendment analysis, it posits that, "The critical question … is whether the collection of personal information aggregated by officers during a given investigation violates reasonable expectations of privacy."[144]

In *United States v. Warshak*, the Sixth Circuit found that the warrantless search of approximately 27,000 emails violated a suspect's reasonable expectation of privacy, even though the emails were stored by a third party service provider.[145] By 2010, email had become an indispensable form of communication, and the Court noted, "Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place."[146] The Court began its examination of the Fourth Amendment interests at stake with the "bedrock principle" announced by the

[142] Michael Goodwin, *A National Security Puzzle: Mosaic Theory and the First Amendment Right of Access in the Federal Courts*, 32 HASTINGS COMM. & ENT. L.J. 179, 180-81 (2010).
[143] *Id.* at 187.
[144] Gray & Citron, *supra* note 31, at 90.
[145] United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).
[146] *Id.* at 284.

Supreme Court in *Kyllo* that "evolving technology must not be permitted to 'erode the privacy guaranteed by the Fourth Amendment.'"[147]

Beginning with the Supreme Court's precedents with regard to mail and telephone conversations, the Sixth Circuit engaged in a function-based analysis of an individual's reasonable expectation of privacy in email messages. It cited protection for the contents of mail and that "*Katz* has … come to stand for the broad proposition that, in many contexts, the government infringes a reasonable expectation of privacy when it surreptitiously intercepts a telephone call through electronic means."[148] So, the court reasoned, "Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."[149] It explained that it would defy reasonable expectations of privacy to insist that a new form of communication serving a very similar purpose as an older one receives different protection based solely on the technical details of communication. "As some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that arise."[150] *Warshak* held that the Fourth Amendment requires a technology-neutral approach and that the function of an emerging technology can

[147] *Id.* at 285 (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).
[148] *Id.*
[149] *Id.* at 285-86. *See Smith*, 442 U.S. at 746, 99 S.Ct. 2577 (Stewart, J., dissenting) ("[S]ince *Katz*, it has been abundantly clear that telephone conversations are fully protected by the Fourth and Fourteenth Amendments.")."
[150] *Warshak*, 631 F.3d at 286. *See Warshak I*, 490 F.3d at 473 ("It goes without saying that like the telephone earlier in our history, e-mail is an ever-increasing mode of private communication, and protecting shared communications through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past.")."

provide the basis for analogizing to established mediums to define a reasonable expectation of privacy.[151]

In *U.S. v. Maynard*, later heard on appeal by the Supreme Court as *U.S. v. Jones*, the D.C. Circuit explicitly embraced the Mosaic Theory.[152] As discussed above, the police had attached a GPS device to a suspect's car which recorded location data for over four weeks. The D.C. Circuit noted that in *United States v. Knotts*, "the [Supreme] Court specifically reserved the question whether a warrant would be required in a case involving 'twenty-four hour surveillance,' stating 'if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.'"[153] The D.C. Circuit found that the privacy interest in the *Knotts* short-term GPS tracking situation was constitutionally distinguishable from the long-term tracking at issue in *Maynard*. Citing *Reporters Committee*, the court held that "[t]he whole of one's movements over the course of a month . . . like a rap sheet . . . reveals far more than the individual movements

[151] The Sixth Circuit used the function of the technology to determine the proper analogy for parties involved and the rights at stake. *Warshak*, 631 F.3d at 286 ("If we accept that an email is analogous to a letter or a phone call, 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. An ISP is the intermediary that makes email communication possible. Emails must pass through an ISP's servers to reach their intended recipient. Thus, the ISP is the functional equivalent of a post office or a telephone company. As we have discussed above, the police may not storm the post office and intercept a letter, and they are likewise forbidden from using the phone system to make a clandestine recording of a telephone call—unless they get a warrant, that is. It only stands to reason that, if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception.").

[152] United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) *aff'd* in part *sub nom.* United States v. Jones, 132 S. Ct. 945 (2012) ("As with the 'mosaic theory' often invoked by the Government in cases involving national security information, 'What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene.' Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble.") (quoting Central Intelligence Agency v. Sims, 471 U.S. 159, 178 (1985).

[153] *Id.* at 556 (quoting United States v. Knotts, 460 U.S. 276, 382-84 (1983)).

it comprises."[154] The fact that the suspect's location could, at any time within those four weeks, have been observed by a police officer without a warrant, is not dispositive of the existence of a Fourth Amendment search. "A reasonable person does not expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how long he stays there; rather, he expects each of those movements to remain 'disconnected and anonymous.'"[155] Although it was affirmed based on different reasoning by the Supreme Court in *Jones*, *Maynard* is an example of a very influential circuit court rejecting the third party doctrine.

The decisions in *Maynard, Warshak* and *Reporters Committee* paved the way for five Justices of the Supreme Court to reject the basic assumptions of the third party doctrine in *Jones*. But upsetting the third party doctrine means something must replace it. Many have pointed out that for all its flaws, the doctrine gives courts a metric to make Fourth Amendment decisions. Mosaic Theory, although very important for its descriptive power and for addressing a central problem of the third party doctrine, gives courts little guidance on when a reasonable expectation of privacy exists.

c. SUMMARY

The third party doctrine developed through a logical jurisprudential process, but it has important limitations. The doctrine was constructed by analogy from the idea that criminals assumed the risk that their comrades were wearing a wire. Each step applying the premise to new facts was derived from the idea that criminals could not hide behind

[154] *Id.* at 551-52.
[155] *Id.* at 553.

technology to suppress evidence that otherwise would have been obtainable through constitutionally sound law enforcement methods. From the conclusion that a suspect assumes the risk that a confidante will betray him, a later court reasoned that a suspect assumed that same risk when he entrusted records to a business. Similarly, the reasoning goes, a phone number that would otherwise have been shared with a human operator constitutes no greater a Fourth Amendment intrusion when recorded by a pen register instead. In this way, supporters of the third party doctrine have argued that it is technology-neutral.

However, as one scholar noted, "[I]t is dubious to justify the Third Party Doctrine on the grounds of technological neutrality when technology causes ever more personal information to be subject to its vacuum."[156] And that is the contradiction of the argument that this doctrine is technology-neutral. It is technology-neutral in form, but not in effect. In other words, under the doctrine, across every medium and technology, there is no reasonable expectation of privacy in information transmitted to third parties. But for every new medium or technology, this may mean something completely different. To have no expectation of privacy in the information shared with a third party when sending a letter through the mail means that the government may collect the names, addresses and date on the envelope without a warrant. To have no expectation of privacy in the information shared with a third party when sending an email from a smart phone may mean the government may collect the names, addresses and time of sending, along with the content of the email, the sender's exact location, IP address and more. What may have

[156] Henderson, *supra* note 14, at 45.

been sent in a letter 50 years ago is now send in an email.[157] But the effect of the third party doctrine is to make one of those expressions protected by the Fourth Amendment and one not. This is how the doctrine is technology-neutral in form, but not effect.

Applying this doctrine to new technologies will often substitute strict adherence to a rule for consideration of its constitutional implications. Although *Smith* made a broad pronouncement of a legal rule, courts must recognize the technology-specific reasoning of that opinion. The conclusion in *Smith* can be reconciled with the implications for personal privacy raised by modern technology, but only through a technology-neutral doctrine rather than mechanical application of the third party doctrine.

Those who defend the third party doctrine almost invariably point to one alleged strength: clarity of application. Putting aside the fact that clarity alone is a totally insufficient justification for defining constitutional rights,[158] the doctrine does not provide such clarity. Proponents of the doctrine point out that the police need clarity about what they can and cannot search without a warrant, and conclude that the bright line distinctions of the third party doctrine provide this clarity.[159] Although a full application of the doctrine would provide clarity, courts are confronting fact patterns, such as *Jones* and *Warshak*, in which the doctrine's conclusions are simply too out of step with reasonable expectations to control the issue.[160] Courts have therefore rejected the doctrine

---

[157] *See* United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010) ("Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place.")

[158] Atwater v. City of Lago Vista, 532 U.S. 318, 366 (2001) (O'Connor, J., concurring) ("While clarity is certainly a value worthy of consideration in our Fourth Amendment jurisprudence, it by no means trumps the values of liberty and privacy at the heart of the Amendment's protections.").

[159] *See, e.g., The Case for the Third Party Doctrine*, *supra* note 379, at 581-83.

[160] *See* Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 642 (2011) ("Apparently aware of the sweeping implications of

as applied to those facts. When courts refuse to adhere to the doctrine, law enforcement does not have the clarity promised by defenders of the doctrine. The third party doctrine simply cannot deliver the clarity its advocates promise in a technological environment so out of step with privacy expectations that courts refuse to adhere to it. The value of clarity is defeated if it is imposed by a test which courts cannot apply to the difficult cases.

This section has provided some examples of Fourth Amendment problems created by emerging technology. As explored further below, such issues will continue to arise with increasing frequency.[161] The third party doctrine was developed based on the premise that a reasonable person would understand that revealing information to a third party waived her privacy interest in it.[162] Whether or not this ever was categorically true, the decisions in *Jones, Warshak* and other cases found it is no longer.

The variety and complexity of technological forms through which people store and communicate information must change Fourth Amendment analysis. Courts can no longer place such immense importance on technical details of which many users may not even be aware.[163] In cases such as *Jones* and *Warshak*, courts have looked to the past capabilities of law enforcement to evaluate where to draw the modern Fourth Amendment line. Specifically they considered how searches made possible by new technology compared in potential scope and invasiveness with older techniques. The

---

a blunderbuss approach to surveillance of digital intermediary records, these courts are increasingly disinclined to take a simplistic and aggressive third party doctrine approach.").

[161] *Infra* Part III.b.iii.1.

[162] *Infra* Part II.b.ii.

[163] *See infra* Part III.b.iii.2; Riley v. California, 134 S. Ct. 2473, 2490 (2014) (citing Brief for Electronic Privacy Information Center, No. 13–132, at 12–14, 20) ("[C]ell phone users often may not know whether particular information is stored on the device or in the cloud").

modern Fourth Amendment requires a technology-neutral solution which takes these considerations into account.

III. CHILLING EFFECTS AND MODERN SURVEILLANCE

a. LITERATURE REVIEW

Fourth Amendment doctrine creates the legal environment in which citizens exercise their First Amendment rights. When the government restricts First Amendment rights indirectly, it nonetheless burdens those rights, and courts have been particularly responsive to chilling effects on First Amendment rights.[164] According to First Amendment scholar Frederick Schauer, "A chilling effect occurs when individuals seeking to engage in activity protected by the [F]irst [A]mendment are deterred from so doing by governmental regulation not specifically directed at that protected activity."[165]

This section explores the chilling effects associated with modern surveillance. In order to do so, it is necessary to define the scope of that surveillance. Different forms of surveillance may impose different chilling effects. For instance, U.S government surveillance has evolved over the past century. After World War II, the Cold War-era government escalated programs of politically targeted surveillance. FBI investigations targeted civil rights leaders such as Martin Luther King, Jr.[166] and "the entire spectrum of [] social and labor movement[s] in the country."[167] These were not criminal

---

[164] Note, *The Chilling Effect in Constitutional Law*, 69 COLUM. L. REV. 808, 809 (1969).
[165] Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the "Chilling Effect,"* 58 B.U. L. REV. 685, 693 (1978).
[166] Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities Report, S. REP. NO. 94-775, 94th Cong., 2d Sess., Book III, at 631 (1976) [hereinafter "Church Report"].
[167] *Id.* at 630 (internal quotation marks omitted).

investigations but rather surveillance for "pure intelligence" purposes.[168] After the Watergate and COINTELPRO scandals and the Church Committee report exploring and condemning the intelligence agencies' abuses,[169] U.S. policy shifted away from explicitly political targeted surveillance.

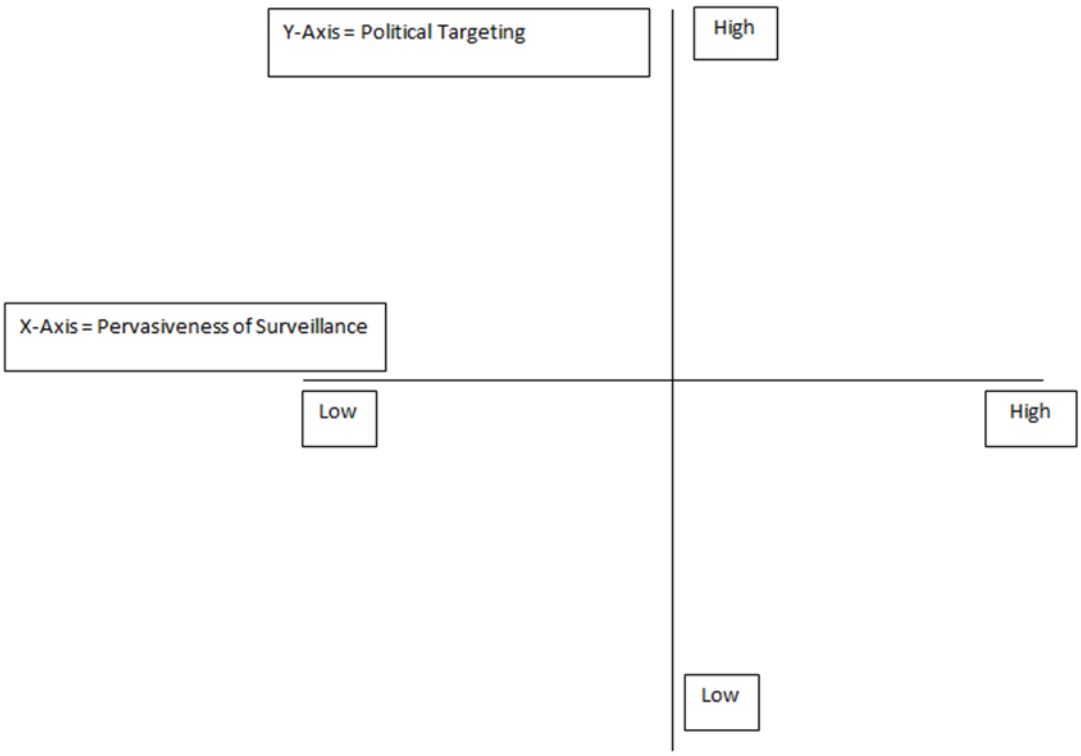
In most cases, government surveillance for the sole purpose of recording political speech is banned in the U.S. For instance, the Privacy Act generally restricts federal agencies from "describing how an individual exercises rights guaranteed by the First Amendment" unless they are "pertinent to and within the scope of an authorized law enforcement activity."[170] Many legal authorities enabling surveillance, such as the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333, also restrict the government's ability to surveil people based on First Amendment-protected activities.[171] Although this does not mean that it does not take place, the government generally cannot target political expression except in the context of a legitimate law enforcement investigation.[172] Below is a set of axes charting ideal types of government surveillance.

---

[168] *Id.*
[169] *Id.*
[170] 5 U.S.C.A. § 552a(e)(7) (West). *See* JAMES O'REILLY, 2 FED. INFO. DISCL. § 22:84 ("The Privacy Act, with limited exceptions, prohibits agencies from maintaining records 'describing how any individual exercises rights guaranteed by the First Amendment.' The Act clearly prohibits even the mere collection of such a record, independent of the agency's maintenance, use, or dissemination of it thereafter.")
[171] 50 U.S.C. § 1805(a)(2)(A) (2012) (FISA provisions stating "[t]hat no United States person may be considered a foreign power or an agent of a foreign power [and therefore subject to lawful surveillance under FISA] solely upon the basis of activities protected by the [F]irst [A]mendment."); In re Production of Tangible Things, Docket No. BR 08-13 (FISA Ct. Feb. 17, 2009), Memorandum of the United States in Response to the Court's Order Dated Jan. 28, 2009, *available at* https://www.aclu.org/files/assets/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf ("[T]argeting a US person solely on the basis of protected First Amendment activities would be inappropriate.").
[172] Clarkson v. I.R.S., 678 F.2d 1368, 1374 (11th Cir. 1982) ("Congress did not intend to dilute the guarantees of the First Amendment by authorizing the maintenance of files on 'persons who are merely exercising their constitutional rights.'").

Figure A

Government Surveillance Ideal Types



In the top-left quadrant are regimes using targeted, politically motivated surveillance. An example would be the FBI in the mid-20th century United States.[173] In the bottom-left quadrant are regimes that perform little surveillance with low political targeting. An example would be early-2000s Greece, which according to a 2007 Privacy International/EPIC report conducted little surveillance and had significant safeguards against targeting in place.[174] In the top-right quadrant are regimes that perform pervasive surveillance and use that surveillance to target political dissidents for further surveillance

[173] *See* NELSON BLACKSTOCK, COINTELPRO: THE FBI'S SECRET WAR ON POLITICAL FREEDOM (1988).
[174] PRIVACY INTERNATIONAL, GREECE: THE 2007 INTERNATIONAL PRIVACY RANKINGS *(2007), available at* https://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559597.

or legal consequences. An example would be modern China.[175] In the bottom-right quadrant are regimes that conduct pervasive surveillance and use that surveillance for non-political targeting purposes such as law enforcement and counterterrorism. An example is the present-day United Kingdom.[176]

Social science research has generally focused on the harms of targeted surveillance. First Amendment scholars have identified the damaging effects of surveillance targeting political dissidents or other nonconformist groups.[177] Such surveillance imposes a number of societal harms, including discouraging unorthodox ideas and stigmatizing those associated with the surveillance.[178]

A foundational 1972 article entitled "Surveillance: The Social Science Perspective" stated, "Surveillance, in American society, is traditionally reserved for those individuals and groups which in some way are presumed to be engaged in illegitimate activities."[179] The effects of this type of surveillance are profound. Targeted surveillance redefines the targets as illegitimate, leading to several harmful consequences.[180] It chills the targeted group and those who sympathize or identify with them by creating a fear of sanctions.[181] Particularly where a regime is known to target political opposition, targeted surveillance can create both a reasonable fear of persecution and mark the target's beliefs as officially disfavored. Such surveillance can stigmatize this group and what it stands

---

[175] *See* Rebecca MacKinnon, *China's "Networked Authoritarianism*," 22 J. DEMOCRACY 32 (2011).
[176] *See United Kingdom,* OPEN NET INITIATIVE (Dec. 18, 2010), https://opennet.net/research/profiles/united-kingdom.
[177] *See, e.g.*, Brian Krueger, *Government Surveillance and Political Participation on the Internet*, 23 SOC. SCI. COMPUTER REV. 439, 442 (2005).
[178] Amory Starr, et al., *The Impact of Surveillance on the Exercise of Political Rights: An Interdisciplinary Analysis 1998-2006*, 31 QUALITATIVE SOC. 251, 255 (2008).
[179] Frank Askin, *Surveillance: The Social Science Perspective*, 4 COLUM. HUM. RTS. L. REV. 59, 65 (1972).
[180] *Id.* at 66.
[181] *Id.* at 64.

for, chilling others from exploring similar beliefs.[182] It can also breed a broader societal intolerance for dissent, infecting the culture and leading to "citizen oppression of other citizens who were labeled non-conformists."[183] Scholars have documented surveillance chilling lawful political activities in places ranging from the USSR[184] to Central America.[185] By targeting political opponents, governments can achieve dual objectives of collecting information and suppressing opposition.

Legal exploration of chilling effects has also largely focused on targeted surveillance. Fear of targeted, political surveillance is well-documented in legal opinions and literature. In 1972, the Supreme Court held that "[C]onstitutional protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs."[186] And in a 1963 case, it stated that protection against surveillance and resulting stigmatization is "all the more essential … where the challenged privacy is that of persons espousing beliefs already unpopular with their neighbors and the deterrent and 'chilling' effect on the free exercise of constitutionally enshrined rights of free speech, expression, and association is consequently the more immediate and substantial."[187] The Court confronted the threat of surveillance as it then existed and this threat was primarily the targeted, stigmatic harms described above.

---

[182] *Id.* at 66.
[183] *Id.* at 67. *See also* Herbert Hyman, *England and America: Climate of Tolerance and Intolerance*, *in* THE RADICAL RIGHT (D. Bell ed. 1963).
[184] Donna Bahry & Brian Silver, *Intimidation and the Symbolic Uses of Terror in the USSR*. 81 AM. POLITICAL SCI. REV. 1065 (1987).
[185] John Booth & Patricia Richard, *Repression, Participation and Democratic Norms in Urban Central America,* 40 AM. J. OF POLITICAL SCI. 1205 (1996).
[186] United States v. United States Dist. Court, 407 U.S. 297, 314 (1972).
[187] Gibson v. Florida Legislative Investigation Comm., 372 U.S. 539, 556-57 (1963).

Fourth Amendment scholarship has likewise focused on these types of harms. The focus has often been on the chilling effects caused by individual searches inflicting stigmatic harm.[188] Many have also explored the harms surveillance can inflict on particular racial or religious groups. For example, one scholar found, "By targeting a particular race for surveillance, investigation, and interrogation, the government brands members of that race as discredited and inherently suspect."[189] This focus on targeted surveillance makes sense because, until the last few decades, searches were necessarily of an individual or a small group. When Fourth Amendment scholars have explored chilling effects, the harms are often conceptualized as being tied to improper retaliation.[190]

However, these studies do not address key aspects about the current state of lawful U.S. surveillance. As technology changes in the ways explored further below, the nature of surveillance is changing.[191] The ideal type and approximate reality of U.S. surveillance belongs in the bottom-right quadrant of the Figure A above, as pervasive, non-political surveillance.[192]

This reveals an important gap in much of the commentary on surveillance. Much of the research tying politically-targeted surveillance to a chilling effect provides little information on key modern surveillance issues. Many of the harms most explored by

---

[188] *See* Alexander A. Reinert, *Public Interest(s) and Fourth Amendment Enforcement*, 2010 U. ILL. L. REV. 1461, 1485-91 (2010).
[189] Thomas Healy, *Stigmatic Harm and Standing*, 92 IOWA L. REV. 417, 484 (2007).
[190] *See* 1 JAMES CARR & PATRICIA BELLIA, LAW OF ELECTRONIC SURVEILLANCE § 2:58 (2014).
[191] *See infra* III.b.ii.
[192] For the purpose of this evaluation, I accept the premise that surveillance by the federal government is not intended to suppress dissent or discourage political opposition. Many would argue that this is a flawed premise. Many of the groups most likely to face intense surveillance efforts, such as Muslims and poor African-Americans, are politically marginalized and underrepresented. Whether this provides a motivation for surveillance, or merely allows the government to pursue the practice with lesser political repercussions, it is difficult to view this overlap as a coincidence. However, the U.S. government is far less likely than other regimes to take action against political dissidents based on purely political actions. Thus although there are clearly political elements, U.S. surveillance can be categorized as low for political targeting.

social scientists, courts and legal scholars are not relevant to pervasive surveillance, as this does not inflict stigmatic injuries. But this type of surveillance can cause other injuries and chill constitutionally protected acts in other ways. In order to inform legal choices, this section will evaluate what chilling effects are genuinely at stake when courts craft a modern Fourth Amendment standard. That is, how does pervasive, non-politically targeted surveillance chill First Amendment activities?

This is not meant to suggest that there is no literature on pervasive surveillance. Both in scholarship and popular culture, pervasive surveillance has long been linked to suppression of expression. From Bentham's panopticon[193] to Orwell's Big Brother,[194] there are salient examples of total surveillance as a powerful mechanism of deterrence and control.

Some scholars have concluded that the legal possibility of indiscriminate surveillance creates a reasonable fear of that surveillance. As one scholar states, "Where such extensive surveillance occurs, or is reasonably feared, the potential for limiting speech is clear: 'There is only one way to guard against [eavesdropping], and that is to keep one's mouth shut on all occasions.'"[195] This section will explore social science research on the chilling effects of indiscriminate surveillance in greater depth. It will analyze efforts to document these chilling effects of indiscriminate surveillance in experimental[196] and real-world[197] settings. It will then seek to examine consequences of

[193] MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 201 (1979).
[194] GEORGE ORWELL, 1984 6-10 (1949).
[195] CARR & BELLIA, *supra* note 190, at § 2:58 (quoting Lopez v. U.S., 373 U.S. 427, 450 (1963) (Brennan, J., dissenting)).
[196] Gregory L. White & Philip G. Zimbardo, *The Effects of Threat of Surveillance and Actual Sureillance on Expressed Opinions Toward Marijuana*, 111 J. SOC. PSYCHOL. 49, 59 (1980).

these effects in light of the massive changes in communication, data production and data storage in the last few decades.

Finally, a great deal of the legal literature about First Amendment chilling effects relates to whether or not these chilling effects are sufficient to confer standing for plaintiffs to challenge surveillance practices. Standing doctrine is a limitation on federal courts derived from Article III of the constitution, requiring that courts hear only cases in which litigants have a true personal stake in the outcome based on a particularized injury in fact.[198] In *Laird v. Tatum*, the Supreme Court heard a challenge to U.S. Army surveillance at political meetings, but ruled that the chilling effects alleged by the plaintiffs did not constitute a judicially cognizable injury.[199] The plaintiffs had not made a sufficiently certain "claim of specific present objective harm or a threat of specific future harm."[200] Similarly, in *Clapper v. Amnesty International*, the Court held that plaintiffs alleging their expression was chilled by government surveillance of their international communication could not allege with sufficient certainty that they were being surveilled under the challenged laws.[201]

These decisions have spurred a glut of literature evaluating the narrow legal question of whether such plaintiffs can ever establish standing and if so, in what circumstances. Articles criticizing *Laird* and *Clapper* have argued that these opinions failed to give proper weight to plaintiffs' claims that surveillance did demonstrably and

---

[197] Alex Marthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior* (Aug. 28, 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564.
[198] CHARLES ALAN WRIGHT, ET AL., § 3531 IN GENERAL, 13A FED. PRAC. & PROC. JURIS. § 3531 (3D ED.).
[199] Laird v. Tatum, 408 U.S. 1, 3 (1972).
[200] *Id.* at 11.
[201] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

concretely affect the exercise of their rights.[202] Scholars have noted that surveillance is often conducted in secret and if plaintiffs cannot prove that they were surveilled individually, it may be impossible to challenge such programs. Neil Richards states, "Plaintiffs can only challenge secret government surveillance they can prove, but the government isn't telling. Plaintiffs (and perhaps civil liberties) are out of luck."[203] However, this scholarship addresses a different problem than the chilling effects issues explored in this thesis. Whether or not chilling effects create standing for plaintiffs to bring a case is a separate issue from how chilling effects should inform Fourth Amendment analysis in criminal cases.

b. ANALYSIS

This section seeks to demonstrate the significance of First Amendment chilling effects for Fourth Amendment law in several steps. First, it will show that Courts have recognized these effects are a significant threat to free expression. Second, it will make evident that Fourth Amendment law must be the basis for protecting against chilling effects. Third, it will examine the multidisciplinary research relevant to the First Amendment problems imposed by modern surveillance and explain how this research can inform Fourth Amendment law. And finally, it will demonstrate how the immense changes in technology, and the pace of those changes, have made pervasive surveillance

[202] Eric Lardiere, *The Justiciability and Constitutionality of Political Intelligence Gathering*, 30 UCLA L. REV. 976, 1035 (1983) ("[A]lthough *Laird* may have been an appropriate exercise of discretion when decided, it does not provide, and indeed prevents, adequate and enduring protection for first amendment rights."); Lexi Rubow, *Standing in the Way of Privacy Protections: The Argument for A Relaxed Article III Standing Requirement for Constitutional and Statutory Causes of Action,* 29 BERKELEY TECH. L. J. 1007, 1018 (2014).
[203] Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1944 (2013).

of far more aspects of people's lives possible, making the potential chilling effects far greater than in the past.

The Supreme Court has recognized how the protection of privacy is often a necessary condition for free expression. In *Bartnicki v. Vopper*, the Supreme Court ruled that the wiretap statute prohibiting disclosure of illegally intercepted communications violated the First Amendment as applied to a defendant publishing information of public concern who had not participated in the interception of the communication.[204] The case required balancing two "interests of the highest order," "protecting privacy and promoting speech."[205] Although the Court ruled that this publication could not be punished, each opinion recognized the central role of privacy in enhancing speech, and the harmful chilling effects that violations of privacy could impose.

The plurality noted the speech interests on both sides of this issue. The wiretap law's "restrictions are intended to protect [privacy], thereby 'encouraging the uninhibited exchange of ideas and information among private parties."[206] The plurality specifically noted that fear of having one's private communications intercepted can chill that First Amendment-protected speech. "In a democratic society privacy of communication is essential if citizens are to think and act creatively and constructively. Fear or suspicion that one's speech is being monitored by a stranger, *even without the reality of such activity,* can have a seriously inhibiting effect upon the willingness to voice critical and

[204] 532 U.S. 514 (2001).
[205] *Id.* at 538 (Breyer, J., concurring).
[206] *Id.* at 532.

constructive ideas."[207] A realistic fear of surveillance, even where no surveillance is taking place, can squelch free thought and open communication.

The concurring and dissenting opinions explored more deeply how chilling effects impact speech. Justice Breyer's concurrence dubbed the wiretap law's effort to safeguard private communications a "speech-enhancing" protection.[208] He argued that privacy is a mechanism to overcome the natural reluctance to speak about personal or controversial issues.[209] If privacy is not protected, these conversations may never take place.[210] Justice Rehnquist's dissent addressed these chilling effects even more directly. Intrusions on private telephone conversations "chill[] the speech of millions of Americans who rely upon electronic technology to communicate each day."[211] This surveillance had the potential to chill private speech not because of the content of the speech, but because of the erosion to the speaker's belief that she could communicate without being intercepted. The *Bartnicki* case presented a difficult fact pattern with persuasive First Amendment interests on both sides. The Court had to balance the right to communicate privately against the right of speakers to publish truthful information. Despite that the Court found the publication was protected, the opinions in that case documented the chilling effects imposed when people cannot feel secure in their private communications.

The Supreme Court more recently recognized that chilling effects can and must be part of the equation in Fourth Amendment law. As Justice Sotomayor stated in *Jones,*

---

[207] *Id.* at 533 (quoting PRESIDENT'S COMMISSION ON LAW ENFORCEMENT AND ADMINISTRATION OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY 202 (1967)).
[208] *Id.* at 536 (Breyer, J., concurring).
[209] *Id.* at 537 (Breyer, J., concurring).
[210] *Id.* (Breyer, J., concurring).
[211] *Id.* at 542 (Rehnquist, J., dissenting).

"Awareness that the Government may be watching chills associational and expressive freedoms."[212] This problem, she argued, could require a change in Fourth Amendment doctrine, including revision of the third party doctrine.[213] And in its 2014 decision in *Riley v. California*, the Court required a warrant to search cell phones incident to an arrest, citing Sotomayor's concurrence for support.[214] The Court observed that Internet search history and GPS location data could reveal significant, private information, and thus a warrantless search of this information required different Fourth Amendment analysis than the court had applied in the past.[215] Although the situation in *Riley*, a search incident to an arrest, is not governed by the third party doctrine, this case reflects the Court's recognition that the changing capabilities of technology have First Amendment and Fourth Amendment implications.

The Court's jurisprudence regarding standing in the context of chilling effects in no way undermines the importance of the issue as a matter of policy. These rulings do not state that the harm at issue is not significant or that it is not implicated by government actions. Rather, in these cases the plaintiffs simply had not stated a particularized, certainly impeding harm fairly traceable to government actions.[216] Many policy debates present issues that do not create a case or controversy under Article III of the constitution.[217] Cases denying standing should not be misinterpreted as denying the significance of chilling effects as a constitutional problem. Cases like *Riley, Jones* and

[212] United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).
[213] *Id.*
[214] Riley v. California, 134 S. Ct. 2473, 2490 (2014) (citing *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).
[215] *Id.*
[216] For an exploration of how a plaintiff could establish standing based on chilling effects to challenge a surveillance program, *see* Lardiere, *supra* note 202.
[217] U.S. CONST. Art. III. (outlining the power delegated the judicial branch of the United States).

Bartnicki illustrate the Supreme Court's recognition of the importance of chilling effects as a policy consideration.

i. The Fourth Amendment as Guardian of the First

Underlying the discussion of chilling effects is the more basic concept of how two sets of constitutional rights, freedom from unreasonable searches and freedom of expression, depend on each other. This section will focus on how the freedom from unreasonable searches has and must act as a guardian of free expression. As a result of the combination of technological development and legal decisions, Fourth Amendment law must play this role, or First Amendment rights will be eroded.

Zurcher v. Stanford Daily,[218] decided by the Supreme Court in 1978, created a concept called the Coextensivity Doctrine.[219] This is the idea the First Amendment protections given to private information are coextensive with the Fourth Amendment protections, meaning that a valid warrant cannot be challenged based on the First Amendment value on the information searched.[220] This doctrine has profound consequences for First Amendment rights by essentially making the protection of those rights dependent on Fourth Amendment rights.

In *Zurcher*, the Stanford University student newspaper challenged a search of its newsroom for photographs of protestors pursuant to a warrant.[221] The Supreme Court confronted the question of whether the First Amendment interests at stake in the search of

---

[218] 436 U.S. 547, 564 (1978).
[219] See, e.g., Suzanne Berger, *Searches of Private Papers: Incorporating First Amendment Principles Into the Determination of Objective Reasonableness*, 51 FORDHAM L. REV. 967, 979 (1983).
[220] *Id.*
[221] *Zurcher*, 436 U.S. at 551.

a newsroom could override a properly issued search warrant supported by probable cause that the premises contained evidence of a crime, even where the occupier of the premises was not involved in the crime. The Court found that a probable cause-supported search warrant was sufficient to protect the First Amendment interests so long as the warrant requirements were met with "scrupulous exactitude."[222] "No more than this is required," the Court held. "Properly administered, the preconditions for the warrant—probable cause, specificity with respect to the place to be searched and the things to be seized, and overall reasonableness—should afford sufficient protection against the harms that are assuredly threatened by warrants for search newspaper offices." [223] The First Amendment rights at stake were protected by the warrant, and if the warrant was properly issued, the First Amendment provided no additional protection.[224] According to one scholar, "*Zurcher* ultimately stands for the proposition that when First Amendment values are at stake, the Fourth Amendment, when properly applied, can adequately protect these values and no further safeguards are needed."[225] Although this sweeping proposition may not apply in all circumstances, *Zurcher* demonstrates how courts can understand Fourth Amendment protections as sufficient to protect First Amendment rights.

In *Reporters Committee for Freedom of the Press v. AT&T*, the D.C. Circuit Court of Appeals expanded on the Coextensivity Doctrine. The court rejected a challenge by

---

[222] *Id.* at 564 (quoting Stanford v. Texas, 379 U.S. 476, 485 (1965).
[223] *Id.* at 565.
[224] The press rights at stake in *Zurcher* were largely protected by the subsequent passage of the Privacy Protection Act of 1980, 42 U.S.C. § 2000 *et seq.* (2000).
[225] Caitlin Thistle, *A First Amendment Breach: The National Security Agency's Electronic Surveillance Program*, 38 SETON HALL L. REV. 1197, 1223 (2008).

journalists to collection of their phone metadata.[226] Expanding on *Zurcher*, the court found that even collections methods that did not require a warrant approved by a neutral magistrate, such as collection of metadata, could not be challenged on First Amendment grounds if they comported with the Fourth Amendment. The majority held that "the First Amendment does not guarantee a journalist, or any other citizen, the freedom to collect information immune from [g]ood faith criminal investigation by means which accord with Fourth and Fifth Amendment protections."[227] The D.C. Circuit went on to expound upon the relationship between First and Fourth Amendment protections. The court found that the Supreme Court, in cases such as *Zurcher*, had declared that "the First Amendment offers no procedural or substantive protections against good faith criminal investigative activity beyond that afforded by the Fourth and Fifth Amendments."[228]

Although these cases rejected the First Amendment as an independent grounds to challenges searches, they were correctly decided and ultimately important in protecting First Amendment rights. First, creating this type of First Amendment attack on a search would do little for the rights of average citizens. These challenges were brought by media organizations. They represent an easily-segregable group which could make an argument on behalf of its rights. The plaintiffs in these cases sought a right based on their role as journalists that would require a greater showing of cause than would be required for surveillance of a private citizen.

Another problem is that asking courts to consider the First Amendment value of the individual's communications, rather than the medium more broadly, will not

[226] Reporters Comm. for Freedom of Press v. Am. Tel. & Tel. Co., 593 F.2d 1030 (D.C. Cir. 1978).
[227] *Id.* at 1054.
[228] *Id. Contra id.* at 1080 (Wright, J., dissenting).

adequately protect speech interests. Weighing a party's First Amendment interests in surveillance information on a case-by-case basis is simply not a reasonable or effective method of protecting these rights. An example is instructive. Imagine that the police hope to surveil an organization they suspect is committing crimes. The police serve a third-party subpoena for the organization's email records. If the organization is not committing crimes, the police will likely find no pattern of suspicious emails. Although the collection may constitute an undue burden on this organization's First Amendment rights, and the government's ability to collect the emails without a warrant may chill expression, there is never any opportunity to challenge it.

If the police do find a suspicious pattern and eventually use this evidence at trial, only then would those in the organization have an opportunity to challenge the collection of these records. Because this standard is evaluated on an individual case basis, the defendants would then be in a position of asking a judge to suppress relevant evidence against them in a criminal case, collected otherwise properly under the Fourth Amendment, based on its tendency to chill their First Amendment rights. Meanwhile, that same information is alleged to be demonstrative of their crimes. Rare indeed would be the judge who suppresses evidence of a crime based solely on the argument that such evidence is protected by the First Amendment.

This process is very different from a normal suppression argument. In a standard Fourth Amendment suppression hearing, occurring only in the context of criminal proceedings against the defendant, the question is whether the government followed its own standards. In a Fourth Amendment suppression context, a party's argument is

essentially "this type of information cannot be collected by the government in this way." If the argument relied on the First Amendment value of the information to that individual, the argument is essentially "my information is particularly valuable and is entitled to heightened protection." This difference illustrates the difficulty of relying on case by case First Amendment analysis.

The Coextensivity Doctrine creates the compelling need for First Amendment values to inform Fourth Amendment analysis. The right to be free from unreasonable searches must encompass protection for freedom of expression, rather than forcing courts to exclude evidence based on independent First Amendment grounds. For reasons explored further below, modern surveillance creates different, greater and more pervasive chills on expression ever before. Unless courts consider these effects by crafting Fourth Amendment standards that take into account the impact of the standard on First Amendment interests, "[r]ights declared in words [may] be lost in reality."[229]

ii. Pervasive Surveillance Creates Chilling Effects

Legal scholars must begin to make use of social science research on the effects of pervasive, non-political surveillance. Research demonstrates that these chilling effects can occur without the stigmatization effects relevant to targeted surveillance. Additionally, when people believe they are being watched, chilling effects can result regardless of whether they truly are. Other studies show that individuals' expression and even thoughts can be altered by the threat of surveillance, regardless of whether there is any punishment truly at stake. When surveillance of an activity is or legally could be

[229] Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting).

pervasive in a society, that activity may be chilled. The studies examined below can provide a basis for courts' analysis of chilling effects in the modern Fourth Amendment context.

The feasibility of pervasive data collection creates uncertainty as to whether one's behavior is being observed. Significantly, "studies demonstrate that even the suggestion of being watched can have a strong impact on human behavior and that change in behavior may be involuntary and subconscious."[230]

Researchers have even found that the threat of surveillance, even if it is later rescinded, can "exert[] a powerful influence over behavior, beliefs, and feelings, whether or not that threat is realized."[231] In a 1980 experiment, students were asked to state their views about punishments for marijuana possession.[232] Of students who were told a video recording of their statements would be given to police for training purposes, only 44% advocated for legalization, while 73% of students who were told that only the researchers would see the tape advocated for legalization.[233] This suggests a strong chilling effect of government surveillance on protected speech. Meanwhile, another group was initially told that their views would be recorded and provided to police, but then were told the camera was broken, so they would not be recorded for the police.[234] These participants still advocated for legalization at a lower rate and showed other indications of remaining influenced by the threat of surveillance.[235] Significantly, after the experiment,

---

[230] Margot Kaminski and Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 UNIV. RICHMOND L. REV. 465, 491 (2014).
[231] White & Zimbardo, *supra* note 196, at 59.
[232] *Id.* at 51.
[233] *Id.* at 58.
[234] *Id.* at 53.
[235] *Id.* at 58-59.

participants reported that they stated their views honestly.[236] The participants did not believe their willingness to express their idea was affected. But it was. The effect of both actual and threatened surveillance was to change the honest beliefs of the participants on this issue. Not only the participants' expressions, but their thoughts, were affected merely by the unfulfilled threat of surveillance.

Even where people do not believe their actions are illegal or subject to punishment, fear of surveillance can create a powerful chill. Social science evidence "is strong enough to conclude that widespread surveillance, or even the belief in it, is damaging to the development of diverse viewpoints, without any *additional clear threat of injury or retaliation*."[237] Even if people do not expect disfavor based on a dissenting viewpoint, their expression and even ideas can be chilled by surveillance.

More recent studies have found similar effects caused by pervasive electronic surveillance. The Helsinki Privacy Experiment studied the impact of ubiquitous surveillance over a six month period.[238] Ten households were equipped with a myriad of surveillance equipment, including cameras and devices logging activity on computers and smartphones.[239] Participants reported several different kinds of behavior change following to the surveillance, including reductions in Internet use and participation in civil organizations, and no longer using anonymous online forums as they would no longer be truly anonymous.[240]

---

[236] *Id*. at 58.
[237] Kaminski, *supra* note 230, at 499 (italics added).
[238] Antti Oulasvirta, et al., *Long-term Effects of Ubiquitous Surveillance in the Home*, *in* PROCEEDINGS OF THE 2012 ACM CONFERENCE ON UBIQUITOUS COMPUTING 41, 41 (2012).
[239] *Id*.
[240] *Id*. at 48.

A 2014 study by a Master's degree candidate at the University of Kent found that "online surveillance [] has behaviour changing effects that inhibit individuals from speaking and writing freely on the Internet."[241] The study was based on an online survey of 1137 German residents measuring their attitudes, behavior and knowledge with respect to indiscriminate online surveillance.[242] The portion relating to chilling effects asked participants if they "avoided writing or speaking about particular topics [], if they had changed their online behaviour [] and other questions regarding violation of privacy, scope and approval of surveillance."[243] The study concluded that "when people worry about being surveilled online and are aware of being watched by intelligence agencies or other governmental institutions, they refrain from acting illegally. However, this behavioural confinement extends onto legal but controversial (i.e. not conform to the government's opinion) topics and practices in order to circumvent reprisal."[244] A chilling effect was most strongly correlated with concern about online surveillance, and was significant regardless of whether the participant identified with the groups they believed were being surveilled.[245]

The study suggested that one way governments could avoid these chilling effects is by creating a transparent legal process that could assure citizens they were not the

---

[241] Johannes Nau, "*Why Protest? I've Got Nothing To Hide" Collective Action Against and Chilling Effects of Internet Mass Surveillance*, 36 (Aug. 2014) (unpublished Master's Thesis, University of Kent), *available at* https://www.academia.edu/9795304/_Why_protest_I_ve_got_nothing_to_hide_Collective_Action_against_and_Chilling_Effects_of_Internet_Mass_Surveillance.

[242] *Id*. at 1. The survey had a large and demographically varied sample, although a limitation is that the sample was much more educated than the general public. *Id.* at 22. Another obvious limitation for application in this thesis is that participants were 95% German. *Id.*

[243] *Id*. at 23

[244] *Id*. at 36

[245] *Id*. at 32

subject of surveillance. "By making sure that espionage techniques are exclusively used on criminals and terrorists and that this procedure is regulated by independent public courts, intelligence agencies could regain the trust of citizens, thereby decreasing the negative psychological effects of Internet surveillance."[246] This study suggests that concern about surveillance leads to chilling effects, but sufficient legal protections can counteract this harm.

A 2014 article entitled "Government Surveillance and Internet Search Behavior" examined the effect of widespread knowledge of Internet search tracking by the NSA program PRISM on Internet searches by individuals.[247] The study tracked the usage on Google's search engine of several hundred different search terms. The data set was derived from "Google Trends, which is a public source of cross-national search volume for particular search terms."[248] These included a set of "suspicious" search terms relating to national security, established by a survey as "likely to get you in trouble with the US government," a set of potentially embarrassing terms, established by a survey as "likely to get you in trouble with a friend," and a control set of Google's top 50 search terms.[249] The study measured the usage of these terms before and after the PRISM disclosures, seeking to understand how the knowledge of this type of Internet surveillance can affect behavior.[250]

The results found a significant chilling of Internet search behavior. After the PRISM disclosures, searches in the U.S. categorized as "likely to get you in trouble with

[246] *Id.* at 22
[247] Marthews & Tucker, *supra* note 197.
[248] *Id.* at 6.
[249] *Id.* at 7-12.
[250] *Id.* at 5.

the U.S. government," fell by about 5%, a "highly significant" statistical finding.[251] These search terms were generally not political in nature. Rather they related to emergency and threat terms, for example, "chemical burn," "hazmat" or "pipe bomb."[252] The PRISM disclosures also decreased Google users' willingness to seek information on personal issues. Though the effect was not seen in the US-only data, the total data set including international searches also found a significant decrease in those searches "likely to get you in trouble with a friend."[253]

The study demonstrates a real-world, empirical impact of pervasive surveillance. The individuals in this data set—that is, all Google users—have no reason to suspect they are a target of individualized surveillance. They have no reason to fear particularized attention from the government. Rather, the awareness of pervasive Internet surveillance has created self-censorship in this data set. Users' expression was chilled as to controversial topics in both national security and personal affairs. These results demonstrate the profound threat to expression posed by pervasive surveillance. The study population was not targeted and the chill was not the result of stigmatization. Rather the general population was significantly less likely to explore controversial topics on the Internet.[254]

Because this study used real-world data, there is obviously no control group, which imposes limitations on the findings. However the authors took several measures to

---

[251] *Id.* at 16.
[252] *Id.* at 28-29.
[253] *Id.* at 16.
[254] There are, of course, limitations to this study. Chilling effects are notoriously difficult to measure empirically. *See* Leslie Kendrick, *Speech, Intent and the Chilling Effect*, 54 WM. & MARY L. REV. 1633, 1653 (2013). Also, the study documents only "the effects of revelations about government surveillance as opposed to the direct effects of government surveillance *per se*." Marthews & Tucker, *supra* note 197, at 24.

verify the robustness of their findings and reduce the potential that other factors created the change in search habits. First, they used a widely varying set of search terms, making it unlikely that another news event would cause a large increase or decrease in searches across the data set.[255] They also analyzed the data in a narrower time frame and the effects were still present "using only data from five weeks before and five weeks after the first surveillance revelations on June 6, 2013."[256] The authors also compared the results to data from 2012 and concluded seasonality was not a major factor.[257]

Other surveys have found similar results among specific populations. In 2013, writers' organization PEN American Center surveyed its world-wide members.[258] It found over the past two years, 24% "avoided writing or speaking about a particular topic" and 25% "Deliberately steered clear of certain topics in personal phone conversations or email messages" because they were concerned their communications were being monitored.[259] Polls in the United States,[260] Germany[261] and Norway[262] found some residents reported changing their online behavior due to surveillance concerns after the first Snowden revelations.

No matter how well intentioned surveillance efforts are or how effectively retribution is limited only to those engaging in illegal actions, the threat of pervasive

---

[255] Marthews & Tucker, *supra* note 197, at 17.
[256] *Id*.
[257] *Id.* at 17-18.
[258] PEN AMERICA, CHILLING EFFECTS: NSA SURVEILLANCE DRIVES U.S. WRITERS TO SELF-CENSOR (2013).
[259] *Id.* at 28, 30.
[260] Stephen Cobb, *NSA and Wall Street: Online Activity Shrinks, Changes Post-Snowden*, WE LIVE SECURITY (Nov. 4, 2013), http://www.welivesecurity.com/2013/11/04/nsa-wall-street-online-activity-shrinks-post-snowden/.
[261] *Ein Jahr nach den Snowden-Enthüllungen*, DIVSI (May 23, 2014), https://www.divsi.de/wp-content/uploads/2014/05/DIVSI-PM-SNOWDEN_2014-05-23.pdf.
[262] PERSONVERN TILSTAND OG TRENDER, NDPA (2014), https://www.datatilsynet.no/Global/04_planer_rapporter/Persovern_tilstandogtrender_2014.pdf.

surveillance has a chilling effect on lawful, constitutionally protected actions and expression. Social science research demonstrates that pervasive surveillance fundamentally causes harms that must be considered in any discussion of its efficacy.

iii. Technology and Modern Surveillance

The changes in technology over the past several decades have created fundamental changes in what surveillance is capable of capturing. Rapid shifts in communication and personal habits have made more pervasive surveillance possible. Changes in government technology have reduced barriers to mass collection. The effects of surveillance explored above, combined with the technological changes explored below, mean that these changes could have profound implications for the relationship between citizens and government.

If the Fourth Amendment is to continue to protect privacy and to safeguard expression, the law must adapt to these changes. Technological development has created significant challenges for Fourth Amendment law. First, the impact of these changes underscores the need for technology-centered approach. As technology changes more quickly and, in turn, alters people's basic habits more quickly, the Fourth Amendment cannot evaluate expectations of privacy based on technical details. Second, technology has transformed the capabilities of surveillance so as to threaten free expression in ways previously unimaginable. The scope of surveillance and the elimination of barriers to pervasive data collection mean that expression is implicated in Fourth Amendment cases as never before.

1. New Technologies Are Being Adopted More Rapidly Than In the Past

The relationship between people and personal technology has changed. In turn, this has altered the relationship between the First and Fourth Amendments. As Chief Justice Roberts notes in the introductory quotation, Fourth Amendment standards are designed in light of the technology of the time. For much of American history, violating someone's privacy required a trespass onto their land or property. Thus Fourth Amendment theory could make use of this physical demarcation.[263] And only long after this premise—that a physical trespass was the only meaningful invasion of privacy—became anachronistic did the court alter its approach in *Katz*.[264] Adjusting to the current technological era presents a formidable judicial challenge. Technology and, perhaps more significantly, mainstream adoption of new technologies are now changing more quickly than ever before.[265] Standards based on the details of a technology can become obsolete as quickly as they are developed. This trend means that courts need a technology-centered approach that can apply to emerging technologies.

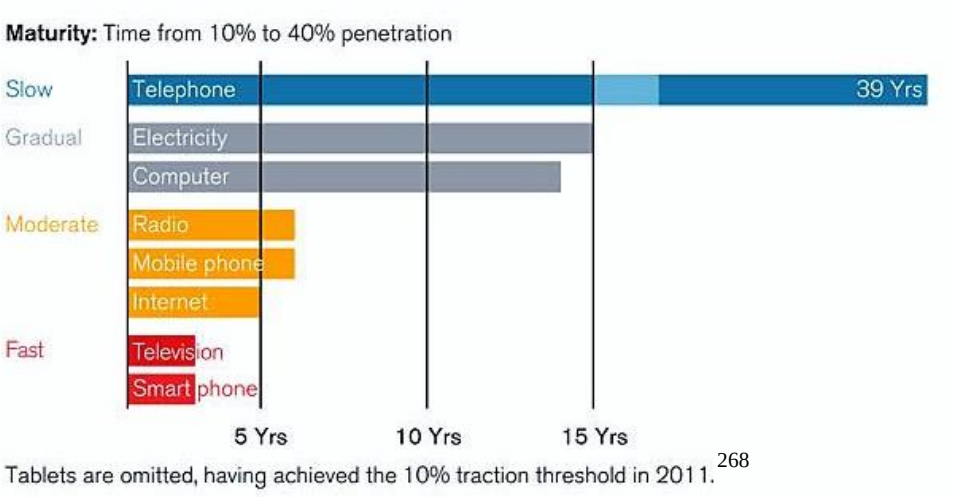
The smartphone is a prime example of the speed of modern technological advance. The mobile, Internet-equipped smartphone is perhaps the single most quickly-adopted technology in history. Smartphones "have also outpaced nearly any comparable technology in the leap to *mainstream* use."[266] For example, "[i]t took landline telephones

[263] *See* Olmstead v. United States, 277 U.S. 438, 466 (1928).
[264] *See* Katz v. United States, 389 U.S. 347, 359 (1967); *Olmstead*, 277 U.S. 438 at 473 (Brandeis, J., dissenting).
[265] When evaluating present circumstances, there is always the threat of recency bias and the exciting, but sometimes mistaken idea that the present is an exception to the past. The data presented in this section addresses this concern, but the tendency towards historical exceptionalism is always a problem in this type of analysis.
[266] DeGusta, *supra* note 72.

about 45 years to get from 5 percent to 50 percent penetration among U.S. households, and mobile phones took around seven years to reach a similar proportion of consumers."[267] Below is a chart demonstrating the amount of time required for various technologies to go from peripheral use (>10%) to mainstream use (<40%). In addition to smartphones, mobile phones and Internet access rank among the technologies most quickly adopted into mainstream use.

Figure B

Rate of Technology Adoption



Tablets are omitted, having achieved the 10% traction threshold in 2011.[268]

As of 2014, 58% of American adults owned smartphones.[269] Though smartphones are only one of many technological changes that significantly affect people's everyday lives, they illustrate both the pace and impact of this evolution.[270]

---

[267] *Id.*
[268] *Id.*
[269] *Mobile Technology Fact Sheet*, PEW RESEARCH CTR., http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/ (last updated Jan. 2015).

Smartphones demonstrate how new technologies can change the capabilities of electronic surveillance. These devices have changed the dynamics of how people communicate, which can be seen most starkly in trends among young people. Between 2009 and 2011, coinciding with the rise of the smartphone, the number of U.S. teens who talked on the phone with friends daily dropped from 38% to 26% and the number who talked in person outside of school dropped from 33% to 25%.[271] Meanwhile, by 2011, 63% of teens exchanged text messages with friends daily and 29%, more than the number who exchanged phone calls or talked in person, exchanged messages on social media.[272]

These changes are one of many examples of Americans' rapidly changing personal habits. Recently-developed technologies now facilitate a great deal of peoples' communication. However, they can also facilitate surveillance of these communications. The potential of these changes to chill expression, particularly given that the pace of changes makes it difficult for courts or legislatures to keep up, will be explored further below. But additionally, such changes raise problems for those who distinguish between forms of communication based on technical details. If communication via social media is replacing communication via a voice call, do reasonable expectations justify treating these communications differently under the Fourth Amendment?

---

[270] Notably, recent technological advances like the Internet, mobile phones and tablets are also among the most quickly adopted. *Id.*
[271] Amanda Lenhart, *Communication Choices,* PEW RESEARCH CTR. (Mar. 19, 2012), http://www.pewinternet.org/2012/03/19/communication-choices/.
[272] *Id.*

2. More of People's Lives Are Mediated Through Technology

As explored above, the way people communicate, and the mediums through which they communicate, are changing more quickly than ever before. Because of current Fourth Amendment law, these changes in habits have potentially profound legal consequences. For instance, while surveillance of telephone communication require a warrant, emails, social media messaging and other electronic forms of communication lack definitive constitutional protection from warrantless collection.[273] The proliferation of methods of communication for which legal protections are reduced or unsettled exposes a greater amount of communication to potential warrantless collection.

Other actions may be mediated and recorded in less obvious ways. Smartphones contain GPS systems and surveillance methods can track the location of a phone even when it is turned off.[274] The government's authority to collect GPS location data without a warrant remains a disputed legal question,[275] but traditional third party doctrine principles would allow for this collection. In any case, smartphones have rapidly made this sensitive, but not necessarily private information—a person's location—available to those with access to the phone's data as never before.

Lastly, smartphones have encouraged the mediation of people's private notes and thoughts. Smartphones have become incredibly personal, storing varied types of personal information and with a person nearly every waking minute. The Supreme Court has noted

---

[273] Theodoric Meyer, *No Warrant, No Problem: How the Government Can Get Your Digital Data*, PROPUBLICA (June 27, 2014), http://www.propublica.org/special/no-warrant-no-problem-how-the-government-can-still-get-your-digital-data.
[274] Erwin Chimerinsky, *Electronic Privacy and the Law*, speech at William & Mitchell College of Law (Feb. 16, 2015).
[275] *See supra* Part II.b.iii.1.

this fact, stating "nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower."[276] Smartphone users record personal notes, grocery lists and calendars, and this information is often backed up remotely to a cloud storage device. Smartphone apps offer to record everything from sleep patterns[277] to health indictors[278] to menstruation cycles.[279] And while information stored on a hard drive would require a warrant while information stored on a cloud is shared with a third party, "cell phone users often may not know whether particular information is stored on the device or in the cloud."[280] As the Supreme Court recognized in *Riley*, these apps "can form a revealing montage of the user's life."[281] Smartphones offer many advantages, but they can also create data about very personal matters that did not previously exist in any tangible form.

The example of the smartphone illustrates the ways in which changes in consumer technology can change people's everyday habits and how recent advances have done so more quickly than in the past. Conversations that were once ephemeral are now preserved, often on a private company's servers. Movements in public that were once merely observable are now recordable. And personal notes or calendars once scribbled on scraps of paper can now be saved to the cloud. In *Riley*, the Court stated, "Indeed, a cell phone search would typically expose to the government far *more* than the most

---

[276] Riley v. California, 134 S. Ct. 2473, 2490 (2014) (citing HARRIS INTERACTIVE, 2013 MOBILE CONSUMER HABITS STUDY (2013)).
[277] *See, e.g., Sleep Cycle*, SLEEP CYCLE, http://www.sleepcycle.com/ (last visited Mar. 7, 2015).
[278] *See, e.g., Experience WebMD on the Go Via Your Smartphone or Tablet*, WEBMD, http://www.webmd.com/mobile (last visited Mar. 7, 2015).
[279] *See, e.g., Fertility Friend App*, FERTILITY FRIEND, http://www.fertilityfriend.com/iphone/ffmobile.php (last visited Mar. 7, 2015). *See also Riley*, 134 S. Ct. at 2491 (citing Brief for Electronic Privacy Information Center, No. 13–132, at 12–14, 20).
[280] *Riley*, 134 S. Ct. at 2490 (citing Brief for Electronic Privacy Information Center, No. 13–132, at 9).
[281] *Id.*

exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is."[282] Not only is more revealing personal data created, but the way in which it is stored, though it may be irrelevant or even unknown to the user, could make it accessible without a warrant.

The adoption of the technologies that facilitate these basic changes in our information ecosystem has been unprecedented in its speed and breadth.[283] And when these technological changes have the legal impact of making citizens' lives more easily observed by government, the changes can have vast social consequences.[284] As communication, behavior, and even thoughts are recorded and accessible as never before, the threat of chilling people's expressive activities has never been greater. In this way, technology has made First Amendment rights more dependent on Fourth Amendment protections than ever before. The mediation of all these types of data creates the potential for surveillance of a much greater fraction of people's lives.

3. These Changes Create the Potential for Long-Term, Retroactive Surveillance

Another fundamental change brought by these shifts in technology is the drastically increased capability for retroactive collection. An important distinction in surveillance is between proactive surveillance, in which the government begins collecting

[282] *Id.* at 2491.
[283] *See* DeGusta, *supra* note 72.
[284] *See* H. REP. NO. 113-34, 38 (2013) ("While privacy rights are often conceptualized as belonging to individuals, they are also important because they ensure a specifically calibrated balance between the power of individuals on the one hand and the state on the other. When the sphere of life in which individuals enjoy privacy shrinks, the state becomes all the more powerful.").

information by observing a target or collecting contemporaneous information, and retroactive surveillance, in which the government collects information documenting the past.

Police have always been able to acquire intimate information about a person through proactive surveillance. Methods such as observation in plain view, use of undercover informants or keeping tabs on movements could reveal a great deal about a target. Although technological changes make this type of surveillance easier, it has always been feasible. But technological changes have altered the potential for retroactive surveillance entirely. Modern Americans, through interaction with a variety of electronic mediums, create vastly more data about themselves than ever before. For instance, license plate reader systems (LPR) can be mounted on police cars or fixed sites to scan and archive data on any car that passes.[285] Law enforcement agencies and government contractors have been building a massive catalogue of LPR scans with billions of data points.[286] This type of passive, suspicionless data collection creates the potential for far more revealing retroactive surveillance than has ever previously been possible.

As explored above, communication and many other types of personal data are now created through the use of modern technology. For instance, location has always been an observable phenomenon, but it has never before been generated automatically—remotely observable, recordable, and capable of after-the-fact data collection. Similarly, a text message creates a record of information that a phone call does not. An Internet search leaves a record, whereas opening an encyclopedia or some other resource does

[285] *License Plate Recognition Systems*, ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/privacy/licenseplates/ (last visited, Apr. 4, 2015).
[286] *Id.*

not. These are not new types of information, but technology has changed the principles of how this information can be obtained and has created the potential for previously impracticable long-term, retroactive collection.

Moreover, this retroactive surveillance can occur in secret. This can include collection of broad swaths of data, from communications to location to personal notes, through a third party often with no notice to the surveillance target.

The passive creation of data documenting myriad aspects of individuals' lives raised the potential of highly intrusive retroactive surveillance. Courts have begun to recognize that searches of huge databases can be incredibly revealing and therefore the rules governing these searches must evolve in order to comply with the Fourth Amendment.[287] Some types of information, such as location, could previously be collected only prospectively or simultaneously. Some types, such as recorded communications, could sometimes have been obtained retroactively, but as a rule, fewer historical records existed. Moreover, they were less likely to be centrally stored by a third party, making collection much more difficult. Indiscriminate, suspicionless data collection enables warrantless retroactive surveillance that was not possible on a similar scale in the past.

[287] United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir. 2010) ("[O]ver-seizing is an inherent part of the electronic search process and … this will be far more common than in the days of paper records. This calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures.").

4. Electronic Surveillance Eliminates Traditional Limitations on Surveillance

The final major change imposed by technology is the elimination of the practical barriers that constrained state surveillance in the past. As Justice Alito stated in *Jones*, "In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical."[288] When longer or more scrutinizing surveillance required additional man-power, hard choices had to be made about resource allocation and cost/benefit balancing. When a police department dispatched an officer to perform physical surveillance or gather documents, it took that officer away from some other task. This meant physical surveillance had to be rationed and applied judiciously.

Many forms of modern electronic surveillance drastically reduce the marginal costs of collecting information on citizens. As explored in *Jones*, moving from physical location surveillance to remote GPS tracking makes "long-term monitoring relatively easy and cheap."[289] Similarly, collection of telephone metadata, which used to require a pen register for each target, can now be collected, aggregated and analyzed in mass.[290] For methods such as these, collection of each additional individual's information requires only negligibly more resources. These and other changes in technology have changed the fundamental calculations affecting surveillance. Rather than making hard choices about how to use surveillance resources, the government at every level can choose to follow the mantra of the National Security Agency: "Collect it all."[291]

---

[288] United States v. Jones, 132 S. Ct. 945, 963 (2012).
[289] *Id.* at 164.
[290] Klayman v. Obama, 957 F. Supp. 2d 1, 37 (D.D.C. 2013).
[291] Ellen Nakashima & Joby Warrick, *For NSA Chief, Terrorist Threat Drives Passion to 'Collect It All',* WASH. POST. (July 14, 2013), http://www.washingtonpost.com/world/national-security/for-nsa-chief-

The rise of technology enabling covert, retroactive electronic surveillance means that Fourth Amendment law must regulate methods of intrusion far more potent than originally conceived. At the time of the drafting of the constitution, a search of letters could reveal some of one's communications; a search of notes could reveal some of one's thoughts; and perhaps even a "tiny constable"[292] could observe one's actions in public. But there was no possibility that all of these could happen on an ongoing basis, without the knowledge of the observed. For the most part, these types of searches were a discrete event, which was understood by all involved. But now, Justice Brandeis' fear that "[w]ays may someday be developed by which the government, without removing papers from secret drawers, can reproduce them in court," has been realized.[293]

When enhanced electronic surveillance is "cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'"[294] The idea that one's conversations, thoughts and movements could be secretly recorded, potentially without a warrant, threatens the idea that privacy can serve as a protector of free expression.

c. Summary

These technological shifts lead to two conclusions. First, technology neutrality is a necessity in order to develop a consistent legal approach that minimizes chilling effects

---

terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html.

[292] *Jones*, 132 S. Ct. at 958, n. 3.

[293] Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

[294] *Jones*, 132 S. Ct. at 956 (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)).

on free expression. The development of Fourth Amendment law demonstrates repeatedly that technology-specific simply cannot standards to keep pace. For decades, Fourth Amendment law granted the government carte blanche to perform perhaps the quintessential modern invasion of privacy: the warrantless wiretap. What is now regarded as a profound invasion of privacy was legal from the invention of the telephone in the 1870s, to its development into mainstream use in the 1920s and 30s, until the *Katz* decision in 1967. New technology is now being adopted into the mainstream at a rapid and accelerating pace, making the only path to protect these interests a technology-neutral Fourth Amendment standard.

Second, electronic surveillance now threatens to chill more types of expression in ways more pervasive than ever before. An individual's interaction with technology creates records of previously ephemeral words and actions. Such records can often be acquired retroactively, from third parties and without notice to the target. And many of the practical limitations to mass surveillance have been eroded or eliminated. These changes in technology demonstrate that more and more of people's lives are exposed to potential surveillance. This means that the chilling effects scholars have begun to identify as a consequence of indiscriminate surveillance now threaten to affect more actions, expression and ideas than ever before. The Fourth Amendment can and must protect First Amendment interests, or privacy, free expression and free thought will be imperiled.

IV. THE PATH FORWARD: A TECHNOLOGY-CENTERED APPROACH

The previous sections have explored the failings of current Fourth Amendment doctrine and the alarming consequences of these failings. This analysis will add to the growing chorus of dissent regarding search and seizure law and better define precisely how pervasive surveillance creates serious harms. Courts must have a standard by which to judge the novel Fourth Amendment issues that come with modern law enforcement techniques. The heavy lifting of reforming the Fourth Amendment jurisprudence will lie in designing a workable standard to replace it. This section will examine a few ground-breaking proposals that not only critique but offer creative solutions to modern Fourth Amendment problems. It will then expand on these proposals to present an improved framework for Fourth Amendment reform.

a. Mosaic Theory

Mosaic Theory is the recent Fourth Amendment reform proposal that has gained the most traction with scholars and courts.[295] The premise is that information collected through means not considered a Fourth Amendment "search" may be transformed into one when large data sets are aggregated to create a revealing "mosaic" of a person's life.[296] As discussed above, this theory attempts to counteract the problematic implications of the increasing capacity to both collect and integrate information about an individual by setting a threshold limitation on the amount of information that may be

[295] *See infra* Part IV.a.
[296] United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) *aff'd* in part *sub nom*. *Jones*, 132 S. Ct. 945.

collected without a warrant.[297] If law enforcement exceeds this limitation, Fourth Amendment protections kick in and further collection would require a warrant or warrant exception.[298] This theory counters the idea under a theory such as the third party doctrine that a collection method either is or is not a search under the Fourth Amendment, regardless of the amount of information collected.

Mosaic Theory is a foundational model in the legal response to modern surveillance. Under the frame of Mosaic Theory, an increasing number of courts and scholars have recognized that "prolonged surveillance of a person's movements may reveal an intimate picture of his life,"[299] and this recognition is an incredibly important step forward. Changes in technology and habits have changed how the Fourth Amendment protects communication, and Mosaic Theory provides a powerful description of this change.

Although Mosaic Theory has been influential in adapting Fourth Amendment theory to the changes in surveillance and data aggregation, it also has important shortcomings. Its adoption represents a very significant change in approach for courts. The first and perhaps most obvious question is: how much is too much? How will law enforcement lawfully collecting information without a warrant know when they have collected so much data that the collection now constitutes a search? Courts and scholars

[297] Dennis, *supra* note 122, at 748.
[298] *Id*.
[299] *Maynard*, 615 F.3d at 562.

have varied significantly on this question.[300] This is an exceedingly difficult question to answer and will likely require arbitrary line drawing.[301]

Another question is how to understand what information can be combined as part of the same "search." If the information is collected through different methods, should it all be considered part of the same data set when determining whether the mosaic is sufficiently revealing?[302] Does it matter if no one individual has access to the entire data set? What about one unit or one department?

Of course any proposal to fundamentally change an area of the law will have unanswered questions. But Mosaic Theory is particularly problematic because it proposes such a fact specific analysis for determining whether a search has occurred. In other words, the necessity of getting a warrant to continue collecting information will necessarily vary in each case because the mosaic of evidence will be different in each case. This presents important problems for both law enforcement and citizens. Because the mosaic of evidence will be different from case to case, both in the information collected and the methods used to collect it, law enforcement will struggle to predict the Fourth Amendment threshold in each case. This lack of clarity for law enforcement can impose practical confusion and create a greater chance of disrupting prosecutions due to the exclusionary rule.[303]

Second, Mosaic Theory ultimately fails to provide citizens with an assurance of privacy in any of their actions or communications. As discussed above, the fear of

---

[300] *See* Orin S. Kerr, The Mosaic Theory of the Fourth Amendment, 111 MICH. L. REV. 311, 330-31 (2012).
[301] *See Jones*, 132 S. Ct. at 954.
[302] Kerr, *supra* note 300, at 334-35.
[303] *See The Case for the Third Party Doctrine*, *supra* note 9, at 582.

surveillance can have a powerful chill on speech and even thoughts.[304] Mosaic Theory essentially leaves in place the third party doctrine for sporadic or short term surveillance. Although this may reduce the likelihood of a sensitive email or Internet search being surveilled, it remains as a legal possibility. This would continue to compromise privacy and impose harmful chilling effects. Mosaic Theory would prevent law enforcement from collecting a large aggregation of data on an individual. But citizens still have no assurance that their sensitive information will not be collected.

While Mosaic Theory has great descriptive power, it produces more questions than answers. Raising these questions is a building block of Fourth Amendment reform. But as a solution to Fourth Amendment problems, Mosaic Theory is unsatisfactory. It creates uncertainty for law enforcement without ensuring key protections to citizens.

b. The First Amendment as Criminal Procedure[305]

Daniel Solove's *The First Amendment as Criminal Procedure*[306] suggests a novel approach, seeking to expand warrant protections based on the First Amendment value of the targeted information, rather than under the Fourth Amendment. Solove quite persuasively argues for the important role of the First Amendment in protecting interests in privacy, anonymity, dissent and autonomy. Solove states, "A century ago, the Fourth and Fifth Amendments would have significantly restricted government information gathering that involves what I will refer to as 'First Amendment activities'—speech, association, consumption of ideas, political activity, religion, and journalism. But today,

[304] *See supra* Part III.b.ii.
[305] Solove, *supra* note 33.
[306] *Id.*

the Fourth and Fifth Amendments play a much diminished role in these contexts."[307] Rather than attempt to preserve the Fourth Amendment's role in protecting First Amendment interests, Solove argues that the First Amendment should have an independent role in protecting against search and seizure.

The basic proposal is this: surveillance requires judicial approval if "the government information gathering affect[s] activities that fall within the boundaries of the First Amendment" and "it [has] a chilling effect upon such activities."[308] This change would be monumental; it would require a warrant for any government collection of expressive material if it chilled such expression. This approach does not easily integrate into how First Amendment speech is often protected. Generally, Fourth Amendment protections apply regardless of content. As Solove observed, in many cases "A diary and a dishpan are equally protected by the Fourth Amendment."[309] However, where speech constitutes a part of a crime, or is alleged to, it is likely without First Amendment protection. And Solove acknowledges this as one of the limiting principles of this proposal's protections.[310] Where the government would attempt to collect speech based on its criminal content, it would be outside the First Amendment's protection. If law enforcement's ability, under the First Amendment, to access the speech depends on whether the contents constitute part of a crime, the logic becomes circular.

---

[307] *Id.* at 113-14.
[308] *Id.* at 152. To perform such surveillance the government would need to demonstrate before a judge "a significant interest in gathering the information" and "that the manner of collection is narrowly tailored to achieving that interest." *Id.* at 159. These requirements will most likely be satisfied by a warrant. *Id.*
[309] *Id.* at 126.
[310] *Id.* at 153.

Solove's proposals are more of a revolution than a reform in search and seizure law. Beyond creating new, independent grounds for challenging surveillance, they would serve to reverse long-established precedent on a variety of issues. The holdings of virtually all of the third party doctrine cases would be reversed, with phone records, business records and financial records likely requiring a warrant.[311] Even beyond this, law enforcement would be required to obtain a warrant to force people to testify about another person's First Amendment activities.[312] Seemingly, even statements police overheard while passing on a street corner would be subject to potential suppression as warrantless surveillance. The scope of reform is both refreshingly bold and dangerously sweeping. Although Solove intends to better protect First Amendment interests against modern intrusions, the article does not adequately address the practical challenges of imposing criminal procedure on law enforcement activities.

Solving the diminution of Fourth Amendment protections by creating an independent role for the First Amendment is a stark shift in doctrine. But it is also unlikely to adequately protect these rights. As discussed above, forcing defendants to argue for suppression of evidence collected in accordance with the Fourth Amendment based on independent First Amendment grounds will put those defendants in a very disadvantageous position in the average criminal case.[313]

Although Solove's article may struggle to make the ambitious argument that virtually any First Amendment chilling effect should create a constitutional criminal procedure right, it accomplishes the still-significant task of outlining how the diminished

[311] *Id. at* 168-72. *See supra* Part II.b.iii.
[312] *Id.* at 175.
[313] *See supra* Part III.b.i.

protections of the Fourth Amendment create chilling effects.[314] These chilling effects, as a kind of by-product of the divergence of Fourth Amendment protections from First Amendment-protected information, must play an important role in solving the problems created by this divergence. While much of the discussion of chilling effects focuses on political repercussions or stigmatic harms,[315] Solove's article does recognize that "broad information gathering that is not directly tied to a concrete penalty or consequence…may still chill speech."[316] Solove insists that chilling effects play a direct role in informing what the Fourth Amendment protects.

c. The Technology-Centered Approach

David Gray and Danielle Citron's article *The Right to Quantitative Privacy* seeks to address some of the weaknesses of Mosaic Theory while providing working approach for reigning in mass surveillance.[317] The result is a powerful and important proposal for revisions to search and seizure law. Gray and Citron's article focuses on the role of the Fourth Amendment as a "constitutional bulwark against law enforcement's tendency to engage in broader and ever more intrusive surveillance."[318] This idea recognizes that the Fourth Amendment is the source both of criminal procedure rights for individual defendants, and the relationship between citizens and the state. It therefore emphasizes the importance of preserving the Fourth Amendment as a societal safeguard against surveillance when determining when a search has occurred.

---

[314] *See id.* at 154-56.
[315] *See id.* at 142-51.
[316] *Id.* at 157.
[317] Citron, *supra* note 31.
[318] *Id.* at 69.

The proposal is for a "technology-centered" approach to determining whether the Fourth Amendment protects against a collection method. It focuses on the surveillance potential of the collection technology at issue. The article states,

> "The threshold Fourth Amendment question should be whether a technology has the capacity to facilitate broad and indiscriminate surveillance that intrudes upon reasonable expectations of quantitative privacy by raising the specter of a surveillance state if deployment and use of that technology is left to the unfettered discretion of law enforcement officers or other government agents. If it does not, then the Fourth Amendment imposes no limitations on law enforcement's use of that technology, regardless of how much information officers gather against a particular target in a particular case. By contrast, if it does threaten reasonable expectations of quantitative privacy, then the government's use of that technology amounts to a 'search,' and must be subjected to the crucible of Fourth Amendment reasonableness, including judicially enforced constraints on law enforcement's discretion."[319]

In determining if the Fourth Amendment should apply to a collection technology, courts should consider "(1) the inherent scope of a technology's surveillance capabilities, be they narrow or broad; (2) the technology's scale and scalability; and (3) the costs associated with deploying and using the technology."[320] If the answers to these questions indicate the technology can facilitate broad and indiscriminate surveillance, "granting law enforcement unfettered access to that technology would violate reasonable expectations of quantitative privacy," and such surveillance should be considered a Fourth Amendment search.[321] This proposal wrestles directly with the most disruptive change to government investigative capacity: the development of technologies capable of cheap, indiscriminate surveillance. It makes powerful arguments that this change in approach is

[319] *Id.* at 71-72.
[320] *Id.* at 102.
[321] *Id.*

both warranted by modern technology and ideologically consistent with the foundations of Fourth Amendment law.[322]

As an example, the article applies the method to drone-enabled video surveillance. This method is "highly scalable and increasingly inexpensive, promising an ever-expanding fleet of drones creating an ever-broadening surveillance net in the skies above us."[323] A drone system is capable of broad, indiscriminate and covert surveillance.[324] Even where surveillance is not occurring, "the ambient threat of unlimited surveillance by drones would remain ubiquitous and constant."[325] Thus, generally speaking, such surveillance would implicate the Fourth Amendment.[326] This would not prevent law enforcement drone use, but rather would require a warrant or warrant exception.[327]

d. A Proposal

The third party doctrine has taken a place in Fourth Amendment jurisprudence that is akin to a dictator grudgingly accepted by world governments. Nations recognize that a despot's decisions can be arbitrary and at times oppressive, but this is accepted in the name of maintaining order. Each of the proposals discussed above has flaws. But the technology-centered approach provides a workable path forward that protects individual

[322] *Id.* at 73-82, 92-101.
[323] *Id.* at 106.
[324] *Id.*
[325] *Id.*
[326] *Id.*
[327] Drone-enabled surveillance has been the subject of much recent debate among Fourth Amendment and privacy scholars. *See* DRONES: EYE IN THE SKY, ELECTRONIC PRIVACY INFORMATION CENTER (2014), *available at* https://epic.org/privacy/surveillance/spotlight/1014/drones.html. *Contra* Gregory S. McNeal, Drones and the Fourth Amendment, *Testimony before the U.S. House of Representatives, Committee on the Judiciary*, 113th Cong. 19-31 (2013).

rights and preserves the Fourth Amendment as a pillar of constitutional protection against government overreach.

This thesis proposes to adopt a technology-centered approach that focuses on the potential for a technology to facilitate pervasive, indiscriminate surveillance. Using this approach as the bedrock of Fourth Amendment reform has many strengths. Importantly, it meets the problem imposed by modern surveillance head on. This standard targets a particular threat that current Fourth Amendment law is not adequate to handle: pervasive surveillance. Technologies with the potential for indiscriminate surveillance have changed what information citizens can keep private from the state. This change in constitutional protection can create chilling effects on speech, association and ideas. The solution should match these problems. Both in a broad and narrow sense, the technology-centered approach accomplishes this. Broadly, the approach focuses directly on the changes in technology that have rendered older Fourth Amendment tests insufficient. And more narrowly, the approach provides the principles to parse which new technological methods pose novel problems and which do not.

Technology has changed so that pervasive and indiscriminate surveillance that was previously unthinkable is now quite feasible. The utilization of such surveillance has demonstrable and highly problematic consequences, such as the chilling of expression, and even ideas. Current doctrine fails as applied to these technologies. Therefore, this is what reform should focus on.

i. Balancing Law Enforcement Needs with Changing Technologies

The technology-centered approach is a technology-neutral path forward for Fourth Amendment law to adapt to technological change while preserving law enforcement capabilities. As discussed above, technology neutrality is the idea that the Fourth Amendment exists not to prevent some particular form of invasion, but to guarantee the substantive right from unreasonable search and seizure.[328] This approach recognizes that although the methods available to law enforcement must change with technology, the allowable incursions into citizen's privacy should stay essentially the same. In other words, "the Fourth Amendment [should] permit access to that which technology hides," but also "should protect that which technology exposes."[329] The technology-centered approach accomplishes this by focusing reform on the modern collection methods capable of exposing previously private or practically obscure information on a mass scale, while preserving human investigation methods that do not pose a similar threat.

Additionally, this approach is far more easily adaptable to changing technology while preserving law enforcement capabilities. For example, Mosaic Theory could invalidate investigation tactics long thought to be constitutional. In *Maynard*, the D.C. Circuit held that although the suspect's location could have been observed by a police officer without a warrant, electronic surveillance of his location for several weeks

[328] *See* Katz v. United States, 389 U.S. 347, 359 (1967) ("Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.").
[329] *The Case for the Third Party Doctrine*, *supra* note 9, at 580.

violated his reasonable expectation of privacy.[330] Theoretically, the suspect could have been tailed by police officers in shifts for several weeks. Though it would require a great many more resources than electronic surveillance, it could be done. Police have used such tactics for decades. The problem, then, is saying that merely because the car was continuously observed without a warrant, the Fourth Amendment was violated. This same logic would cut off a traditional police stakeout after a certain amount of time. This is problematic because it makes unconstitutional a traditionally-used method that does not pose any new or novel issue. It makes little sense to argue that physical surveillance that has always been permissible is now unconstitutional, merely because a different way of accomplishing this task enables indiscriminate surveillance.

A strength of the technology-centered approach is that it avoids this incongruity by leaving much of Fourth Amendment law intact. It preserves the central holding of *Katz.* Unlike the Mosaic Theory, it preserves a sequential approach to Fourth Amendment analysis, taking each government action in isolation and asking if at any point law enforcement made use of a means of collection considered a Fourth Amendment search.[331] And more practically, because they would not pose a threat of indiscriminate surveillance, many traditional investigative methods would still be available to law enforcement without obtaining a warrant. A technology-centered approach provides an ideologically consistent way of addressing new problems without disturbing many traditional practices and methods.

---

[330] United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) *aff'd* in part *sub nom*. United States v. Jones, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012).

[331] *See* Kerr, *supra* note 300, at 348 (contrasting the sequential method with the novel probabilistic method proposed by Mosaic Theory).

Consequently, it avoids many of the difficult and perhaps unanswerable questions raised by applying Mosaic Theory. Because Mosaic Theory constrains activity at the point of aggregation rather than collection, it can be difficult to determine what information constitutes part of one data set. If the FBI has a cache of information on an individual, does all of this information make up the mosaic, even if the portions of the information are controlled only by separate units and have never been shared? This question need not be answered under a technology-centered approach because it maintains a sequential analysis. Just as in traditional Fourth Amendment analysis, if each step of collection is legitimate, there is no threat that the whole of a dataset could constitute a violation.

In sum, this "approach would not implicate human surveillance and other traditional investigative techniques."[332] Because human investigation methods do not implicate the danger of indiscriminate, pervasive surveillance and the harms associated with this, it would not be limited by a technology-centered approach and would continue to be governed by current doctrine. One could argue that this focus on technology ignores the potential for a surveillance state powered by human surveillance. As Nazi Germany or many Soviet satellite states demonstrate, the power of invasive, human surveillance can create a powerful chill. But for a variety of reasons, this distinction between human and technological surveillance is significant.[333] Even where it is possible to collect the same information, human methods simply cannot rival electronic collection's capacity for indiscriminate surveillance.

---

[332] Citron, *supra* note 31, at 124.
[333] *See supra* Part III.b.iii.

Additionally, physical surveillance methods provide for greater transparency and political checks. Human observation necessarily requires more overt methods of collection. Where human surveillance increases to the scope that it threatens to create a surveillance state, the necessary resources and physical presence will force a level of public awareness of its presence that may not occur in the case of cheaper, more discreet electronic surveillance.[334] This provides a greater opportunity for a political response to surveillance.

The technology-centered approach better balances the competing interests at the core of the Fourth Amendment. It preserves many traditional methods for which a warrant requirement would significantly restrain the practice of police work. But it recognizes the profound changes in surveillance capacity and responds head on to the societal challenges this creates.

ii. Clarifying "Broad" Surveillance

There are important ways in which the technology-centered approach proposed by Gray and Citron in *The Right to Quantitative Privacy* can be strengthened. Criteria must be provided for distinguishing broad from narrow surveillance. The article provides three main criteria for determining when a technology is capable of scaling to support indiscriminate surveillance: "(1) the inherent scope of a technology's surveillance

[334] The proposal would also create transparency for challenged police methods. When courts analyze a technology for its potential for indiscriminate surveillance, it will be important to understand how it is used. This will require law enforcement to make a showing of the types of surveillance the technology is used for. While of course special procedures could be made such as in camera review for particularly sensitive issues, as a general rule this aspect of the technology-centered approach to Fourth Amendment cases can provide definition to the public's understanding of surveillance technologies.

capabilities, be they narrow or broad; (2) the technology's scale and scalability; and (3) the costs associated with deploying and using the technology."[335] Gray and Citron provide little clarity on how courts are to distinguish "broad" from "narrow" surveillance.

Chilling effects should be considered in this analysis. Chilling effects provide one of the enduring fears about government surveillance and an important way to identify its most pernicious dangers. When a surveillance technology has the potential to create chilling effects, it should be considered "broad" surveillance for at least two reasons. First, such surveillance implicates a wide set of rights implicating not only privacy rights, but also rights of autonomy, free expression and free thought. Second, chilling effects pose a societal harm that can affect even those who are never actually subject to surveillance. Defining how "broad" surveillance is, based only on who is actually surveilled, would ignore an important impact of surveillance: chilling effects on those who fear such surveillance. Chilling effects provide a way to measure the true breadth of the impact of a surveillance technology.

For instance, gunshot locators are a common feature of urban police departments. These systems are often installed in high crime areas.[336] If the system were cheaply scalable to a mass application, would such a system be broad enough to intrude on peoples' quantitative expectations of privacy? The question likely depends on whether this is considered broad or narrow surveillance. It certainly seems less intrusive than other forms of indiscriminate surveillance. But without criteria it may be difficult to

[335] Citron, *supra* note 31, at 102.
[336] Allison Klein, *District Adding Gunfire Sensors*, WASH. POST. (July 5, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/07/04/AR2008070402356.html.

explain why. One significant reason is that these systems are narrowly tailored to avoid chilling lawful behavior. A dense system of microphones that picks up and records all sounds would implicate very different rights than a dense system that merely alerts authorities to the noise of a gunshot. An important way to distinguish these systems is to identify the extent to which they chill the exercise of other rights.

The technology-centered approach also allows for creative legislative solutions to balancing Fourth Amendment rights with law enforcement capabilities. Where legislation acts to blunt some aspects of the technology that made it a threat to reasonable expectations of quantitative privacy, different constitutional analysis can apply. If a technology is capable of broad indiscriminate surveillance, but the possibility has been made legally impermissible by legislation, the evaluation changes. Courts should judge the legally permissible applications of the technology. In this way, the government can take advantage of improving technologies to benefit investigations while limiting the breadth of surveillance to avoid Fourth Amendment challenges. A constitutional problem can be avoided and policies can be clarified if the threat of surveillance is reined in by comprehensive legislation.

iii. Challenges to the Technology-Centered Approach

A primary objection to the technology-centered approach will undoubtedly be that it does not provide sufficiently clear guidelines for law enforcement. The exclusionary rule means that if police invade a suspect's reasonable expectations

of privacy to obtain evidence without a warrant or applicable warrant exception, the evidence generally will be suppressed. If police are unsure how to comply with the Fourth Amendment, it can be harmful for all parties. Suspects may have their Fourth Amendment rights violated (suppression of the resulting evidence only partially ameliorates this harm), and police waste resources collecting inadmissible evidence. If each new technology requires a judge's evaluation, law enforcement frequently will be either violating the Fourth Amendment or denying themselves allowable investigation techniques out of fear that they may violate the Fourth Amendment.

However, lawmakers can soften the harsh effects of the exclusionary rule by enacting legislation that delineates search rules for law enforcement, allowing evidence obtained in good faith to be presented in court. For example, in *Warshak*, the search of email was found to violate the suspect's reasonable expectation of privacy, but the evidence was not subject to the exclusionary rule because police relied on a good faith interpretation of a federal law.[337] This approach would allow police to use methods they believe to be constitutional without as great a risk of having evidence suppressed, and will allow courts to build precedent without such harsh implications for individual cases.

Critics will no doubt argue that the technology-centered approach changes the focus of Fourth Amendment analysis from intrusion on an the privacy of a particular individual to an evaluation of the broader threat to society as a whole. The argument would point out that an individual who was tracked remotely by a highly sophisticated,

[337] United States v. Warshak, 631 F.3d 266, 292 (6th Cir. 2010).

expensive GPS tracking system may potentially have no recourse, while an individual who was tracked by a cheaper system capable of mass surveillance has had their Fourth Amendment rights violated. This could make an individual's rights dependent on the development of technology that is beyond his or her control and essentially irrelevant to her personal actions. But this "problem" merely reflects the way in which Fourth Amendment analysis has always operated. Under traditional doctrine, law enforcement can often collect information by one means but not another. Police can search a person's home when she is not there with the consent of her housemate, but cannot if the target is home and objects.[338] In determining whether a limited search is permissible, police can consider many factors extraneous to a target's actions, such as presence in a high crime area.[339] Police can invade people's reasonable expectations of privacy based on a warrant exception such as exigency, even if not necessarily created by the target.[340] Fourth Amendment doctrine has always melded individual and societal concerns in determining the proper lines for warrantless searches.

Another similar argument is that discarding the third party doctrine leaves an individual's privacy to the whim of the companies that hold that individual's information. If, for instance, a search of emails required a warrant, an email provider could voluntarily choose to reveal those emails to the government without a warrant. At least as a constitutional matter, this is likely both true and unremarkable. Similarly, for anyone who shares a home with another person, that other individual could consent to a warrantless

[338] Georgia v. Randolph, 547 U.S. 103, 123 (2006).
[339] Illinois v. Wardlow, 528 U.S. 119, 124 (2000).
[340] *See* Bryan M. Abramoske, *It Doesn't Matter What They Intended: The Need for Objective Permissibility Review of Police-Created Exigencies in "Knock and Talk" Investigations,* 41 SUFFOLK U. L. REV. 561, 562 (2008).

search of the home, so long as the other individual was not present to object.[341] Exclusive control has never been a requirement for a physical space to be considered private under the Fourth Amendment, and this should not change merely because the search is of an electronic "space."

e. Summary

The Fourth Amendment does not create a general right to privacy.[342] But it does prohibit "every unjustifiable intrusion by the government upon the privacy of the individual."[343] The Supreme Court made clear in *Katz* that an intrusion is not justified merely because it does not cross an arbitrary technological line. In order to protect against the type of indiscriminate government searches that the Fourth Amendment was designed to prevent, courts must recognize a more adaptable understanding of privacy. The technology-centered approach provides a set of technology-neutral principles for courts to weigh when a search has occurred.

One compelling strength of this proposal is that it is unlikely to satisfy either privacy advocates or law enforcement officials. The standard is decidedly more protective of privacy than the third party doctrine. But under it, many highly revealing traditional methods will not be considered a search. And unlike Mosaic Theory, there is no substantive line the government cannot cross. Lawfully collected information may be integrated and analyzed to reveal a detailed picture of an individual's life. This approach

[341] United States v. Matlock, 415 U.S. 164, 172 (1974) ("[I]t is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched.").
[342] Katz v. United States, 389 U.S. 347, 350 (1967).
[343] Olmstead v. United States, 277 U.S. 438, 478 (1928).

preserves the Fourth Amendment as a shield against pervasive government surveillance while empowering law enforcement to utilize every tool at their discretion.

Although it is important to give law enforcement adequate resources to pursue their mission, the Fourth Amendment is an intentional restriction on this power in the service of broader democratic values. Law enforcement's mission and values will always push for greater ability to investigate crimes, not out of desire to create a police state but because this is the inevitable result of dogged police work. As Justice Brandeis observed, "The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning, but without understanding."[344] The Fourth Amendment is meant to limit the government's power to search and seize, even when this limitation will interfere with investigatory tools. The drafters of the Constitution targeted indiscriminate searches and general warrants precisely because of their power—to reveal and to oppress. To the extent that the technology-centered approach protects against the type of pervasive state intrusion that has been feared since the Constitution's inception, this restriction on the power of law enforcement is intentional and monumentally important.

The technology-centered approach navigates the changes to surveillance capabilities to protect both privacy and expressive rights. The Bill of Rights creates a bulwark between government and the people and preserving dissent and disfavored expression is a central reason for this. Under this approach, courts can weigh the impact on these rights in evaluating surveillance technologies and thus better preserve this bulwark.

[344] *Id.* at 479.

The technology-centered approach undoubtedly has doctrinal challenges. But critics who would raise concerns about clarity for law enforcement must confront the reality of the modern third party doctrine, which cannot deliver the clarity its proponents claim it can.[345] A bright-line standard which courts refuse to apply because it diverges so greatly from common sense does not provide predictability. Leaving courts to follow or reject the third party doctrine on an ad hoc basis, with little theory guiding their decisions when they do, threatens citizens' Fourth Amendment protections without providing consistency. Any test of reasonableness leaves ambiguity, but the American legal system relies on such tests, from tort law to criminal law. The technology-centered approach gives courts the foundation to analyze novel Fourth Amendment questions in a way that better preserves the balance between privacy and expression rights and law enforcement prerogatives.

V. CONCLUSION

The right of privacy is not a right to be free from a list of particular intrusions. But privacy means more than the absence of a wiretap or physical intrusion. It is a right to exclude the state from our lives unless the state can justify the intrusion. Fundamentally, we cannot define this right without reference to the past. A reasonable expectation of privacy is that recognized by a reasonable citizen. People's expectations are informed by the rights that they have enjoyed up to that point. Roughly speaking, people expect that they will continue to enjoy the same rights they have always had, unless there is a good

[345] *See supra* Part II.c.

reason for a change. Simply put, the fact that the government has the technical capability for greater surveillance over its citizens is not a good reason.

Restricting technological surveillance is not about Luddism or artificially hamstringing law enforcement. It is simply another step in the development of a Fourth Amendment law that reflects the problems of the society it protects. As practical limitations on surveillance disappear, the law must play a different role. We now face a constitutional dilemma as Justice Brandeis did in *Olmstead*. Just as he did, today we perceive that past invasions had "been necessarily simple," while today "[s]ubtler and more far-reaching means of invading privacy have become available to the government."[346] And just as he did, courts today must reject the notion that the law will allow this development to fundamentally change the relationship between citizens and their government.

> "The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone-the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[347]

[346] *Olmstead*, 277 U.S. at 473 (Brandeis, J., dissenting).
[347] *Id.* (Brandeis, J., dissenting).

Bibliography

Bryan M. Abramoske, *It Doesn't Matter What They Intended: The Need for Objective Permissibility Review of Police-Created Exigencies in "Knock and Talk" Investigations,* 41 SUFFOLK U. L. REV. 561 (2008).

Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy*", 34 VAND. L. REV. 1289 (1981).

Frank Askin, *Surveillance: The Social Science Perspective,* 4 COLUM. HUM. RTS. L. REV. 59 (1972).

Donna Bahry & Brian Silver, *Intimidation and the Symbolic Uses of Terror in the USSR.* 81 AM. POLITICAL SCI. REV. 1065 (1987).

Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply,* 54 B.C. L. REV. 1 (2013).

Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens,* 72 GEO. WASH. L. REV. 1375 (2004).

Suzanne Berger, *Searches of Private Papers: Incorporating First Amendment Principles Into the Determination of Objective Reasonableness*, 51 FORDHAM L. REV. 967 (1983).

NELSON BLACKSTOCK, COINTELPRO: THE FBI'S SECRET WAR ON POLITICAL FREEDOM (1988).

John Booth & Patricia Richard, *Repression, Participation and Democratic Norms in Urban Central America,* 40 AM. J. OF POLITICAL SCI. 1205 (1996).

Susan Brenner & Leo Clarke, *Fourth Amendment for Shared Privacy Rights in Stored Transactional Data,* 14 J. L. & POL'Y 211 (2006).

1 JAMES CARR & PATRICIA BELLIA, LAW OF ELECTRONIC SURVEILLANCE § 2:58 (2014).

Erwin Chimerinsky, *Electronic Privacy and the Law*, speech at William & Mitchell College of Law (Feb. 16, 2015).

Stephen Cobb, *NSA and Wall Street: Online Activity Shrinks, Changes Post-Snowden*, WE LIVE SECURITY (Nov. 4, 2013), http://www.welivesecurity.com/2013/11/04/nsa-wall-street-online-activity-shrinks-post-snowden/.

Andrew Cohen, *Is the NSA's Spying Constitutional? It Depends on Which Judge You Ask*, THE ATLANTIC (Dec. 27, 2013), http://www.theatlantic.com/national/archive/2013/12/is-the-nsas-spying-constitutional-it-depends-which-judge-you-ask/282672/.

Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119 (2002).

Michael DeGusta, *Are Smart Phones Spreading Faster than Any Technology in Human History?*, M.I.T. TECH. REV. (May 9, 2012), *http://www.technologyreview.com/news/427787/are-smart-phones-spreading-faster-than-any-technology-in-human-history/*.

Erin Smith Dennis, *A Mosaic Shield: Maynard, the Fourth Amdnement, and Privacy Rights in the Digital Age*, 33 CARDOZO L. REV. 737 (2011).

Ein Jahr nach den Snowden-Enthüllungen, DIVSI (May 23, 2014), https://www.divsi.de/wp-content/uploads/2014/05/DIVSI-PM-SNOWDEN_2014-05-23.pdf.

DRONES: EYE IN THE SKY, ELECTRONIC PRIVACY INFORMATION CENTER (2014), *available at* https://epic.org/privacy/surveillance/spotlight/1014/drones.html.

License Plate Recognition Systems, ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/privacy/licenseplates/ (last visited, Apr. 4, 2015).

Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199 (2009).

Fertility Friend App, FERTILITY FRIEND, http://www.fertilityfriend.com/iphone/ffmobile.php (last visited Mar. 7, 2015).

MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON (1979).

Jace Gatewood, *District of Columbia Jones and the Mosaic Theory-in Search of A Public Right of Privacy: The Equilibrium Effect of the Mosaic Theory*, 92 NEB. L. REV. 504 (2014).

Michael Goodwin, *A National Security Puzzle: Mosaic Theory and the First Amendment Right of Access in the Federal Courts*, 32 HASTINGS COMM. & ENT. L.J. 179, (2010).

David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013).

H. REP. NO. 113-34, 38 (2013).

LUKE HARDING, THE SNOWDEN FILES (2014).

HARRIS INTERACTIVE, 2013 MOBILE CONSUMER HABITS STUDY (2013).

Thomas Healy, *Stigmatic Harm and Standing*, 92 IOWA L. REV. 417 (2007).

Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39 (2011).

Herbert Hyman, *England and America: Climate of Tolerance and Intolerance*, *in* THE RADICAL RIGHT (D. Bell ed. 1963).

Ashby Jones, *NSA Judge Is No Stranger To Controversial Rulings*, WALL ST. J. (Dec. 17, 2013), http://online.wsj.com/news/articles/SB10001424052702304403804579264413734088306.

Michael T.E. Kalis, *Ill Suited to the Digital Age: Fourth Amendment Exceptions and Cell Site Location Information Surveillance*, 13 U. PITT. J. TECH. L. POL'Y 1 (2013).

Margot Kaminski and Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 UNIV. RICHMOND L. REV. 465 (2014).

Kenneth Karst, *The Files*: *Legal Controls Over the Accuracy and Accessibility of Stored Personal Data*, 31 LAW & CONTEMP. PROB. 342 (1966).

Allison Klein, *District Adding Gunfire Sensors*, WASH. POST. (July 5, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/07/04/AR2008070402356.html.

Amanda Lenhart, *Communication Choices,* PEW RESEARCH CTR. (Mar. 19, 2012), http://www.pewinternet.org/2012/03/19/communication-choices/.

Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-first Century*, 65 IND. L.J. 549 (1990).

Leslie Kendrick, *Speech, Intent and the Chilling Effect*, 54 WM. & MARY L. REV. 1633 (2013).

Orin Kerr, *Four Models of Fourth Amendment Protection*, STAN. L. REV. 503 (2007).

Orin Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561 (2009).

Orin S. Kerr, *Defending the Third-Party Doctrine: A Response to Epstein and Murphy*, 24 BERKELEY TECH. L.J. 1229 (2009).

Orin S. Kerr, The Mosaic Theory of the Fourth Amendment, 111 MICH. L. REV. 311 (2012).

Brian Krueger, *Government Surveillance and Political Participation on the Internet*, 23 SOC. SCI. COMPUTER REV. 439 (2005).

JACOB LANDYNSKI, SEARCH AND SEIZURE AND THE SUPREME COURT (1966).

Eric Lardiere, *The Justiciability and Constitutionality of Political Intelligence Gathering*, 30 UCLA L. REV. 976 (1983).

Mary Graw Leary, *Katz on A Hot Tin Roof-Saving the Fourth Amendment from Commercial Conditioning by Reviving Voluntariness in Disclosures to Third Parties*, 50 AM. CRIM. L. REV. 341 (2013).

Rebecca MacKinnon, *China's "Networked Authoritarianism*," 22 J. DEMOCRACY 32 (2011).

Alex Marthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior* (Aug. 28, 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564.

Gregory S. McNeal, Drones and the Fourth Amendment, *Testimony before the U.S. House of Representatives, Committee on the Judiciary*, 113th Cong. 19-31 (2013).

Theodoric Meyer, *No Warrant, No Problem: How the Government Can Get Your Digital Data*, PROPUBLICA (June 27, 2014), http://www.propublica.org/special/no-warrant-no-problem-how-the-government-can-still-get-your-digital-data.

M. Blane Michael, *Reading the Fourth Amendment: Guidance from the Mischief That Gave It Birth*, 85 N.Y.U. L. REV. 905 (2010).

Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L. J. 1239 (2009).

Ellen Nakashima & Joby Warrick, *For NSA Chief, Terrorist Threat Drives Passion to 'Collect It All',* WASH. POST. (July 14, 2013), http://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html.

Johannes Nau, "*Why Protest? I've Got Nothing To Hide" Collective Action Against and Chilling Effects of Internet Mass Surveillance* (Aug. 2014) (unpublished Master's Thesis, University of Kent), *available at* https://www.academia.edu/9795304/_Why_protest_I_ve_got_nothing_to_hide_Collective_Action_against_and_Chilling_Effects_of_Internet_Mass_Surveillance.

PERSONVERN TILSTAND OG TRENDER, NDPA (2014), https://www.datatilsynet.no/Global/04_planer_rapporter/Persovern_tilstandogtrender_2014.pdf.

Note, *The Chilling Effect in Constitutional Law*, 69 COLUM. L. REV. 808 (1969).

GEORGE ORWELL, 1984 (1949).

Antti Oulasvirta, et al., *Long-term Effects of Ubiquitous Surveillance in the Home, in* PROCEEDINGS OF THE 2012 ACM CONFERENCE ON UBIQUITOUS COMPUTING 41 (2012).

PEN AMERICA, CHILLING EFFECTS: NSA SURVEILLANCE DRIVES U.S. WRITERS TO SELF-CENSOR (2013).

Mobile Technology Fact Sheet, PEW RESEARCH CTR., http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/ (last updated Jan. 2015).

PRESIDENT'S COMMISSION ON LAW ENFORCEMENT AND ADMINISTRATION OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY (1967).

PRIVACY INTERNATIONAL, GREECE: THE 2007 INTERNATIONAL PRIVACY RANKINGS (2007), *available at* https://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559597.

Privacy Protection Act of 1980, 42 U.S.C. § 2000 *et seq.* (2000).

Blake Ellis Reid, *Substitution Effects: A Problematic Justification for the Third-Party Doctrine of the Fourth Amendment*, 8 J. TELECOMM. & HIGH TECH. L. 613 (2010).

Alexander A. Reinert, *Public Interest(s) and Fourth Amendment Enforcement*, 2010 U. ILL. L. REV. 1461 (2010).

Neil M. Richards, *The Dangers of Surveillance,* 126 HARV. L. REV. 1934 (2013).

John Roberts, Chief Justice, United States Supreme Court, Centennial Lecture Series at Rice University (Oct. 17, 2012), *available at* https://mediacore.rice.edu/media/centennial-lecture-series-a-conversation-with-the-.

Lexi Rubow, *Standing in the Way of Privacy Protections: The Argument for A Relaxed Article III Standing Requirement for Constitutional and Statutory Causes of Action,* 29 BERKELEY TECH. L.J. 1007 (2014).

Julian Sanchez, *The Talking Points for NSA's Dragnet Don't Hold Up*, CATO INSTITUTE (July 24, 2013), http://www.cato.org/blog/talking-points-nsas-dragnet-dont-hold.

Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the "Chilling Effect,"* 58 B.U. L. REV. 685 (1978).

Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 643 (2013).

Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities Report, S. REP. NO. 94-775, 94th Cong., 2d Sess., Book III (1976).

F. SIEBERT, FREEDOM OF THE PRESS IN ENGLAND: 1476-1776 (1952).

Sleep Cycle, SLEEP CYCLE, http://www.sleepcycle.com/ (last visited Mar. 7, 2015).

CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2007).

Daniel Solove, *The First Amendment As Criminal Procedure*, 82 N.Y.U. L. REV. 112 (2007).

Amory Starr, et al., *The Impact of Surveillance on the Exercise of Political Rights: An Interdisciplinary Analysis 1998-2006*, 31 QUALITATIVE SOC. 251 (2008).

Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614 (2011).

Caitlin Thistle, *A First Amendment Breach: The National Security Agency's Electronic Surveillance Program*, 38 SETON HALL L. REV. 1197 (2008).

RICHARD THOMPSON, CONG. RESEARCH SERV., THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE (2014).

United Kingdom, OPEN NET INITIATIVE (Dec. 18, 2010), https://opennet.net/research/profiles/united-kingdom.

Alex Vlisides, *Snowden Leaks Continue to Reveal NSA Surveillance Programs, Drive U.S. and International Protests and Reforms*, SILHA BULLETIN (Dec. 2013), http://www.silha.umn.edu/news/Fall2013/SILHACENTERSnowdencoverstoryUniversityofMinnesota.html.

Experience WebMD on the Go Via Your Smartphone or Tablet, WEBMD, http://www.webmd.com/mobile (last visited Mar. 7, 2015).

Gregory L. White & Philip G. Zimbardo, *The Effects of Threat of Surveillance and Actual Sureillance on Expressed Opinions Toward Marijuana*, 111 J. SOC. PSYCHOL. 49 (1980).

CHARLES ALAN WRIGHT, ET AL., § 3531 IN GENERAL, 13A FED. PRAC. & PROC. JURIS. § 3531 (3D ED.).

Cases Cited

Atwater v. City of Lago Vista, 532 U.S. 318 (2001).

Bartnicki v. Vopper, 532 U.S. 514 (2001).

Berger v. New York, 388 U.S. 41 (1967).

Boyd v. United States, 116 U.S. 616 (1886).

California v. Greenwood, 486 U.S. 35 (1988).

Cent. Intelligence Agency v. Sims, 471 U.S. 159 (1985).

Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

Davis v. United States, 131 S. Ct. 2419 (2011).

Entick v. Carrington and Three Other King's Messengers, 19 HOW. ST. TRI. 1029 (1765).

Ex parte Jackson, 96 U.S. 727 (1878).

Georgia v. Randolph, 547 U.S. 103 (2006).

Gibson v. Florida Legislative Investigation Comm., 372 U.S. 539 (1963).

Hoffa v. United States, 385 U.S. 293 (1966).

Illinois v. Lidster, 540 U.S. 419 (2004).

Illinois v. Wardlow, 528 U.S. 119 (2000).

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

Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013).

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

Laird v. Tatum, 408 U.S. 1 (1972).

Lee v. United States, 343 U.S. 747 (1952).

Lopez v. U.S., 373 U.S. 427 (1963).

Olmstead v. United States, 277 U.S. 438 (1928).

Reporters Comm. for Freedom of Press v. Am. Tel. & Tel. Co., 593 F.2d 1030 (D.C. Cir. 1978).

Riley v. California, 134 S. Ct. 2473 (2014).

Stanford v. Texas, 379 U.S. 476 (1965).

United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010).

United States Dept. of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749 (1989).

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

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

United States v. Matlock, 415 U.S. 164 (1974).

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

United States v. Miller, 425 U.S. 435 (1976).

United States v. United States Dist. Court, 407 U.S. 297 (1972).

United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

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

Weems v. United States, 217 U.S. 349 (1910).

White v. United States, 401 U.S. 745 (1971).

Zurcher v. Stanford Daily, 436 U.S. 547 (1978).