FOURTH AMENDMENT PRAGMATISM

Daniel J. Solove*

Abstract: This Essay argues that the Fourth Amendment reasonable expectation of privacy test should be abandoned. Instead of engaging in a fruitless game of determining whether privacy is invaded, the U.S. Supreme Court should adopt a more pragmatic approach to the Fourth Amendment and directly face the issue of how to regulate government information gathering. There are two central questions in Fourth Amendment analysis: (1) the Coverage Question—does the Fourth Amendment provide protection against a particular form of government information gathering? and (2) the Procedure Question—how should the Fourth Amendment regulate this form of government information gathering? The Coverage Question should be easy to answer: the Fourth Amendment should regulate whenever government information gathering creates problems of reasonable significance. Such a scope of coverage would be broad, and the attention wasted on the Coverage Question would be shifted to the Procedure Question. This pragmatic approach to the Fourth Amendment is consistent with its text and will make Fourth Amendment law coherent and comprehensive.

Introduction

The reasonable expectation of privacy test currently governs the scope of Fourth Amendment protection. Ever since *Katz v. United States* was decided in 1967,[1] the U.S. Supreme Court has determined the boundaries of Fourth Amendment protection against government information gathering by asking whether a person exhibits an "expectation of privacy" that society recognizes as "reasonable."[2]

The reasonable expectation of privacy test has led to a contentious jurisprudence that is riddled with inconsistency and incoherence. Debates rage over whether particular government information gathering

* © 2010, Daniel J. Solove, Professor of Law, George Washington University Law School. I would like to thank Danielle Citron, Thomas Crocker, Deven Desai, Orin Kerr, Raymond Ku, Christopher Slobogin, Michael Sullivan, Brian Tamanaha, and Peter Winn for helpful comments on the manuscript.

[1] 389 U.S. 347, 353 (1967).

[2] *Id.* at 361 (Harlan, J., concurring).

activities invade "privacy."[3] I have been a frequent participant in these discussions, often criticizing judicial decisions under the Fourth Amendment as lacking a progressive understanding of privacy in light of modern technology.[4]

What makes for a great intellectual game does not make for good law. Few commentators are particularly fond of Fourth Amendment law.[5] U.S. Supreme Court decisions applying the reasonable expectation of privacy test have been attacked as "unstable"[6] and "illogical,"[7] and even as engendering "pandemonium."[8] As one commentator has aptly observed, "[M]ost commentators have recognized that regardless of the political palatability of recent decisions, [F]ourth [A]mendment doctrine is in a state of theoretical chaos . . . ."[9]

For a long time, I believed that with the appropriate understanding of privacy—one that is well-adapted to modern technology, nimble and nuanced, forward-looking and sophisticated—Fourth Amendment jurisprudence could be rehabilitated. I now realize I was wrong.

---

[3] *See, e.g.*, Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 Miss. L.J. 1, 71 (2005) (critiquing the Court's conception of privacy as inadequate to deal with new technology); Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 Ind. L.J. 549, 554–55 (1990) ("[W]e should return to the privacy test intended by [Justices] Stewart and Harlan and to the underlying values that motivated it."); Brian J. Serr, *Great Expectations of Privacy: A New Model of Fourth Amendment Protection*, 73 Minn. L. Rev. 583, 642 (1989) ("[T]he Court's current [F]ourth [A]mendment analysis is based on simplistic and logically incorrect theories of public exposure.").

[4] Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age 199–200 (2004) [hereinafter Solove, The Digital Person]; Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083, 1086–87 (2002) ("[*Olmstead v. United States*, 277 U.S. 438 (1928)] symbolizes the Court's lack of responsiveness to new technology, unwarranted formalism in its constitutional interpretation, and failure to see the larger purposes of the Fourth Amendment."); Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. Rev. 112, 126 (2007) ("Due to changes in technology and the realities of modern life, much First Amendment activity now leaves digital fingerprints beyond private zones protected by the Fourth Amendment.").

[5] *See* Gerald G. Ashdown, *The Fourth Amendment and the 'Legitimate Expectation of Privacy*,' 34 Vand. L. Rev. 1289, 1321 (1981); 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); Richard G. Wilkins, *Defining the "Reasonable Expectation of Privacy": An Emerging Tripartite Analysis*, 40 Vand. L. Rev. 1077, 1080 (1987). *But see* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 Stan. L. Rev. 503, 506–07 (2007) ("Scholars and students of Fourth Amendment law find the current approach frustrating because the courts routinely mix and match the four models. . . . But appearances can be deceiving. What at first looks like conceptual confusion turns out to be a much-needed range of approaches.").

[6] Colb, *supra* note 5, at 122.

[7] Ashdown, *supra* note 5, at 1321.

[8] *See* Wilkins, *supra* note 5, at 1081.

[9] Donald R.C. Pongrace, *Stereotypification of the Fourth Amendment's Public/Private Distinction: An Opportunity for Clarity*, 34 Am. U. L. Rev. 1191, 1208 (1985).

The entire debate over reasonable expectations of privacy is futile, for it is not focused on the right question. The debate is reminiscent of the philosophical dispute over a squirrel that William James relates in his book, *Pragmatism:*

> The *corpus* of the dispute was a squirrel—a live squirrel supposed to be clinging to one side of a tree-trunk; while over against the tree's opposite side a human being was imagined to stand. This human witness tries to get sight of the squirrel by moving rapidly round the tree, but no matter how fast he goes, the squirrel moves as fast in the opposite direction, and always keeps the tree between himself and the man, so that never a glimpse of him is caught. The resultant metaphysical problem now is this: *Does the man go round the squirrel or not?* He goes round the tree, sure enough, and the squirrel is on the tree; but does he go round the squirrel?[10]

James told the others that the debate was in vain—it all boiled down to what "going round" the squirrel meant.[11] If "going round" meant passing the squirrel in all four directions, then the man went around the squirrel.[12] But if going around meant being on all four sides of the squirrel, then "the man fails to go round him, for by the compensating movements the squirrel makes, he keeps his belly turned towards the man all the time, and his back turned away."[13] We should avoid getting bogged down in such fruitless debates, James explains, as it is more productive to focus on "practical consequences."[14]

Just as the scholars futilely debated whether the man went around the squirrel, we too have often focused on the wrong question when considering Fourth Amendment protection—whether there is an invasion of privacy. As a result, current Fourth Amendment coverage often bears little relation to the problems caused by government investigative activities. It also bears little relation to whether it is best to have judicial oversight of law enforcement activity, what that oversight should consist of, how much limitation we want to impose on various government information gathering activities, and how we should guard against abuses of power.

---

[10] William James, Pragmatism 22 (Prometheus Books 1991) (1907).
[11] *Id.*
[12] *Id.*
[13] *Id.* at 22–23.
[14] *Id.* at 23.

In this Essay, I argue for a more pragmatic approach to the Fourth Amendment. There are two central questions in Fourth Amendment analysis:

> (1) Does the Fourth Amendment provide protection against a particular form of government information gathering?
>
> (2) How should the Fourth Amendment regulate this form of government information gathering?

I will refer to Question 1 as the "Coverage Question" and Question 2 as the "Procedure Question."

The Coverage Question has preoccupied Fourth Amendment law and has led to a complicated morass of doctrines and theories. We should sidestep the contentious debate about expectations of privacy—or about any other specific value as a trigger for Fourth Amendment protection. Instead, whenever a particular government information gathering activity creates problems of reasonable significance, the Fourth Amendment should require regulation and oversight. These problems not only involve invasion of privacy, but also chilling of free speech, free association, freedom of belief, and consumption of ideas. They can involve inadequately constrained government power, lack of accountability of law enforcement officials, and excessive police discretion, among other things. The Fourth Amendment should provide coverage whenever any of these problems might occur.

Such an approach would result in Fourth Amendment coverage that is comprehensive rather than haphazard. It would be consistent with the Fourth Amendment's language, which speaks broadly in terms of "unreasonable searches."[15] The Coverage Question thus should be easy—the Fourth Amendment should provide protection whenever a problem of reasonable significance can be identified with a particular form of government information gathering.

The more difficult question is the Procedure Question, which involves how the Fourth Amendment should regulate government activities. What kind of regulation would best limit the problems created by a particular government information gathering activity? What degree of oversight would be effective as well as practical? Too much time and energy is wasted on the Coverage Question; it should be redirected to the Procedure Question.

---

[15] *See* U.S. CONST. amend. IV.

In an ideal world, government information gathering would be regulated by a comprehensive statutory regime. Courts would analyze whether the rules in this statutory regime met basic Fourth Amendment principles rather than craft the rules themselves. A pronouncement as short and vague as the Fourth Amendment best serves as a guidepost to evaluate rules, rather than as a source of those rules.

But a comprehensive statutory regime to regulate government information gathering does not yet exist. Statutes regulate government information gathering in isolated areas, but there is no all-inclusive regime.[16] For better or worse, the Fourth Amendment has been thrust into the role of the primary regulatory system of government information gathering. Until there is a substitute, we should treat the Fourth Amendment as the regulatory system it has been tasked with being. If legislatures respond with rules of their own, courts should shift from crafting the rules to evaluating the rules made by legislatures.

In Part I of this Essay, I argue that we should not only jettison the reasonable expectation of privacy test, but also avoid focusing on any specific kind of problem as the trigger for Fourth Amendment protection. Instead, as I contend in Part II, the Fourth Amendment should regulate whenever government information gathering leads to any type of problem of reasonable significance. Rather than constricting the scope of Fourth Amendment protection in arbitrary and illogical ways, courts should directly address how to regulate government information gathering. Toward this end, I propose a way courts can better work with legislatures to develop a comprehensive and balanced regulatory system for government information gathering. The system would be primarily statutory, following the Constitution's guiding principles. I conclude by justifying this approach and defending it against potential objections.

I. The Fourth Amendment's Limited Coverage

A. *A Regulatory System in One Sentence*

Unlike other countries, which have a centralized police system regulated by statute, the United States has a decentralized system of law enforcement that is regulated primarily by the Constitution.[17] The structure of our current regulatory regime for government information gathering is framed largely by the Fourth Amendment, a short pronouncement that says:

---

[16] *See* Solove, The Digital Person, *supra* note 4, at 202–10.

[17] *See id.* at 188.

> 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 [w]arrants shall issue, but upon probable cause, supported by [o]ath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[18]

An elaborate regulatory system rests upon this one sentence. Throngs of judicial decisions interpreting the Fourth Amendment have spawned an extensive body of rules that govern nearly all aspects of government law enforcement investigative activity, such as: engaging in audio and visual surveillance; searching homes, cars, bags, and computers; and establishing checkpoints.

The Framers of the Constitution likely had no idea the Fourth Amendment would serve as the foundation for regulating our entire system of law enforcement. They thought the Constitution only applied to the federal government, which in 1789 played only a minimal role in law enforcement. The Federal Bureau of Investigation, Central Intelligence Agency, National Security Agency, and other federal agencies did not yet exist. State and local police were also very minimal, and they were not governed by the Fourth Amendment.

But in the centuries after 1789, the nature of the Constitution and of law enforcement changed dramatically. The number and size of police forces burgeoned. Nascent technologies gave the government greater power to gather citizens' personal information. New federal government agencies were created to address crime and national security issues. Because comprehensive statutory regulation of law enforcement was lacking at all levels of government, something was needed to regulate what law enforcement officials could do. The U.S. Supreme Court filled the void by crafting an extensive regulatory system based on constitutional law, and the Fourth Amendment became the guiding set of rules for when and how the government could gather information about individuals.

Today, when the Fourth Amendment applies to any particular government information gathering activity, it requires government searches and seizures to be "reasonable."[19] This has been interpreted to mean that government officials typically must obtain a warrant supported by probable cause.[20] Such a process provides the judicial branch some

---

[18] U.S. Const. amend. IV.

[19] Solove, The Digital Person, *supra* note 4, at 189.

[20] *Id.*

oversight of law enforcement officials as warrants must be authorized by a judge before the government may engage in its search.[21] The government must prove that it has probable cause—"reasonably trustworthy information" that is sufficient to "warrant a man of reasonable caution in the belief that an offense has been or is being committed" or that evidence will be found in the place to be searched.[22] When the government fails to follow these procedures, the typical remedy is the "exclusionary rule" under which the information gleaned from the illegal search is excluded from trial.[23]

Many government activities to acquire personal information are not covered by the Fourth Amendment.[24] In this regulatory void, there is sometimes a statute that provides protection, but in many circumstances, there is no protection at all, and the government may act without any oversight or limitation.[25] Therefore, the threshold test to determine whether the Fourth Amendment will regulate a particular government information gathering activity becomes crucial.

B. *The Rise of the Reasonable Expectation of Privacy Test*

What test should be used to determine when the Fourth Amendment will regulate a particular law enforcement activity? For well over a century, the U.S. Supreme Court has wrangled with this question. The Fourth Amendment uses the terms "searches" and "seizures," but it does not define them. Moreover, the language of the Fourth Amendment was written centuries ago, long before modern technology dramatically altered the ways the government can gather information.

The Court's initial answer, formed in the late nineteenth century, was to focus on physical types of intrusions.[26] The Fourth Amendment covered rummaging through people's papers and invading their prop-

---

[21] *Id.*

[22] Brinegar v. United States, 338 U.S. 160, 175–76 (1949).

[23] Mapp v. Ohio, 367 U.S. 643, 654–55 (1961) ("We hold that all evidence obtained by searches and seizures in violation of the Constitution is, by that same authority, inadmissible in a state court.").

[24] *See* Solove, The Digital Person, *supra* note 4, at 200–02 (describing how courts have found no reasonable expectation of privacy where the police viewed the interior of the defendant's greenhouse from a helicopter, where police officers searched garbage bags that the defendant left on the curb, or where information is known or exposed to third parties).

[25] *See id.*

[26] *Id.* at 196–97 ("[T]he Court viewed invasions of privacy as a type of physical incursion.").

erty.[27] Such an approach made sense during this time, for these methods were the primary means by which government officials gathered information about people.

But technology changed everything. Developed in the late nineteenth century, telephone communication—and the ability to wiretap telephone conversations—posed new and challenging Fourth Amendment questions. In 1928, in *Olmstead v. United States*, the U.S. Supreme Court addressed whether wiretapping would be covered by the Fourth Amendment or left unregulated.[28] The Court concluded that the Fourth Amendment did not cover wiretapping because "[t]here was no entry of the houses or offices of the defendants."[29]

Justice Louis Brandeis dissented. He argued that the Court's threshold test for determining Fourth Amendment coverage was myopic and antiquated, and that the Fourth Amendment must have the "capacity of adaptation to a changing world."[30] A more flexible and evolving approach should be used because:

> Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.[31]

It took nearly forty years for the Court to embrace Brandeis's view. In 1967, the Court overruled *Olmstead* in *Katz v. United States*.[32] *Katz* gave birth to the Court's current approach to determining whether the Fourth Amendment applies—the reasonable expectation of privacy

---

[27] *Id.* This was known as the "physical trespass doctrine." *See, e.g.*, Silverman v. United States, 365 U.S. 505, 511–12 (1961) (concluding that use of a "spike mike," which penetrated into the wall of a person's home, constituted a physical trespass and therefore triggered Fourth Amendment protection); Goldman v. United States, 316 U.S. 129, 134 (1942) (holding that the Fourth Amendment does not cover a recording device that does not physically intrude upon one's property).

[28] 277 U.S. 438, 464–66 (1928).

> The United States takes no such care of telegraph or telephone messages as of mailed sealed letters. The Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.

Id.

[29] *Id.* at 464.

[30] *Id.* at 472 (Brandeis, J., dissenting).

[31] *Id.* at 473.

[32] Katz v. United States, 389 U.S. 347, 353 (1967).

test.[33] The purported goal of the reasonable expectation of privacy test was to permit the Fourth Amendment to respond to changing technology.[34] As Professor Carol Steiker has observed, "Brandeis could have felt vindicated by the Court's replacement of the trespass doctrine with one more oriented toward the right of 'privacy.'"[35]

At first glance, the reasonable expectation of privacy test seems quite sensible. According to the Court, "[t]he overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State."[36] Protecting privacy gives the Amendment coherence and a central purpose. It provides guidance about which government information gathering activities should be regulated. It turns the Amendment away from outdated formalistic considerations, such as whether there was a physical trespass, and refocuses it on privacy, a central value for freedom and democracy. The reasonable expectation of privacy test also promises flexibility—it can evolve with society and remain connected to current social values.

But the test has failed to live up to aspirations. Subsequent to the test's development, the Supreme Court adopted a conception of privacy that countless commentators have found to be overly narrow, incoherent, short-sighted, deleterious to liberty, and totally out of touch with society.[37] According to Professor Scott Sundby, "The Fourth Amendment as a privacy-focused doctrine has not fared well with the changing times of an increasingly non-private world and a judicial reluctance to

---

[33] *Id.* at 351–52 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." (citations omitted)).

[34] *Id.*

[35] Carol S. Steiker, *Brandeis in* Olmstead*: "Our Government Is the Potent, the Omnipresent Teacher,"* 79 Miss. L.J. 149, 162 (2009).

[36] Schmerber v. California, 384 U.S. 757, 767 (1966).

[37] *See, e.g.*, Aya Gruber, *Garbage Pails and Puppy Dog Tails: Is That What* Katz *Is Made of?*, 41 U.C. Davis L. Rev. 781, 790 (2008) ("[T]he spirit of *Katz* is a promise of freedom from unwarranted invasions of privacy in all areas we consider intimate. Unfortunately, the *Katz* revolution was not unequivocally liberal."); Katz, *supra* note 3, at 554 (noting that the Court has applied the reasonable expectation of privacy "to reduce rather than enhance [F]ourth [A]mendment protections"); George C. Thomas III, *Time Travel, Hovercrafts, and the Framers: James Madison Sees the Future and Rewrites the Fourth Amendment*, 80 Notre Dame L. Rev. 1451, 1500 (2005) ("The 'expectation of privacy' notion is flawed to the core."). *But see* Peter Winn, Katz *and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 McGeorge L. Rev. 1, 9 (2008) (arguing that the reasonable expectation of privacy test was a way for the Court to incorporate its previous test of physical trespass, which focused on property, within a new approach that was more expansive).

expand individual rights."[38] Professor Morgan Cloud observes that "it is fair to conclude that *Katz* is a failure, at least if its original purpose was to ensure that Fourth Amendment standards regulate the use of modern surveillance technologies."[39]

For example, under the "third party doctrine," the Court has held that there is no reasonable expectation of privacy for the ever-growing amount of personal data maintained by third parties. In 1979, the Court concluded in *Smith v. Maryland* that the Fourth Amendment does not apply to a list of the telephone numbers a person dials.[40] Because people "know that they must convey numerical information to the phone company" and that the phone company records this information for billing purposes, people cannot "harbor any general expectation that the numbers they dial will remain secret."[41] In 1976, in *United States v. Miller*, the Court used similar reasoning to conclude there was no reasonable expectation of privacy in bank records.[42]

Beyond the third party doctrine, the Court has concluded that people lack a reasonable expectation of privacy when the police view their property from a helicopter,[43] search through trash bags left out on the curb,[44] use a dog to sniff luggage for illegal substances,[45] and have an undercover informant secretly record and transmit conversations.[46]

I could go on, listing many more cases and doctrines that I and other commentators find troubling. I have critiqued the Court's con-

---

[38] Scott E. Sundby, *"Everyman"'s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 Colum. L. Rev. 1751, 1771 (1994).

[39] Morgan Cloud, *Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment*, 72 Miss. L.J. 5, 28–29 (2002); *see also* Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. Rev. 741, 769–77 (2008) (arguing that the Fourth Amendment provides insufficient protection against government "relational surveillance" using traffic data).

[40] 442 U.S. 735, 743 (1979).

[41] *Id.*

[42] 425 U.S. 435, 442 (1976).

[43] Florida v. Riley, 488 U.S. 445, 450–52 (1989) ("[Petitioner] could not reasonably have expected that his greenhouse was protected from public or official observation from a helicopter had it been flying within the navigable airspace for fixed-wing aircraft.").

[44] California v. Greenwood, 486 U.S. 35, 43–44 (1988) ("We have already concluded that society as a whole possesses no [reasonable expectation of privacy] with regard to garbage left for collection at the side of a public street.").

[45] Illinois v. Caballes, 543 U.S. 405, 409 (2005) ("[T]he use of a well-trained narcotics-detection dog . . . during a lawful traffic stop, generally does not implicate legitimate privacy interests.").

[46] United States v. White, 401 U.S. 745, 753–54 (1971) (concluding that an agent could record or transmit a conversation with the defendant without a warrant).

ception of privacy as focusing too much on the secrecy of information and failing to account for the fact that in today's Information Age, so little of our data is secret.[47] I long wanted the Court to recognize that it was wrong about privacy. I thought that if the Court were to conceptualize privacy as I recommended, Fourth Amendment law would be revitalized.

I now have come to believe that the reasonable expectation of privacy test cannot be resuscitated. The debate over what constitutes privacy is an important and interesting one—and certainly has relevance for the Fourth Amendment—but it is not the central determination that should trigger Fourth Amendment protection.

C. *Why the Reasonable Expectation of Privacy Test Is Doomed*

The reasonable expectation of privacy test is not merely in need of repair—it is doomed. From the way it is formulated, the test purports to be an empirical metric of societal views on privacy. The Supreme Court, however, has never cited to empirical evidence to support its conclusions about what expectations of privacy society deems to be reasonable. As one commentator has stated: "How do we know what society is prepared to accept as reasonable? Because there is no straightforward answer to this question, 'reasonable' has largely come to mean what a majority of the Supreme Court Justices says is reasonable."[48]

The Court itself has acknowledged that the test is not entirely empirical.[49] For example, in *United States v. Jacobsen*, the Court noted that "[t]he concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation, however well justified, that certain facts will not come to the attention of the authorities."[50] As Justice Scalia once stated, "In my view, the only thing the past three decades have established about the *Katz* test . . . is that, unsurprisingly, [reasonable expectations of privacy] bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable."[51]

---

[47] Solove, The Digital Person, *supra* note 4, at 42–44.

[48] Robert M. Bloom, Searches, Seizures, and Warrants 46 (2003); *see also* Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring).

[49] *See Smith*, 442 U.S. at 740 n.5 ("[W]here an individual's subjective expectations had been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was.").

[50] 466 U.S. 109, 122 (1984).

[51] *Carter*, 525 U.S. at 97 (Scalia, J., concurring).

The Court rarely takes any steps to determine what society deems reasonable. Clearly, the justices have no special ability to sense the collective desires and values of all citizens of the United States. They instead are just stating their own preferences and opinions, whether they are consistent with society's or not.

In many instances, what the Court considers to be an invasion of privacy bears no relationship to what people will say in surveys. Professors Christopher Slobogin and Joseph Schumacher conducted a survey to see if people's expectations of privacy matched what the Court had determined.[52] Their data revealed that "the Supreme Court's conclusions about the scope of the Fourth Amendment are often not in tune with commonly held attitudes about police investigative techniques."[53]

Many commentators critique the Supreme Court for failing to look to the actual societal expectations of privacy.[54] But there are good reasons why the Court refuses to use empirical evidence to identify reasonable expectations of privacy. Taking surveys—a predominant way to measure things empirically—raises several problems. First, various subgroups may differ in their attitudes about privacy. People's attitudes about privacy diverge depending upon their race, ethnicity, or religion. The Bill of Rights has oft been championed as necessary to protect minorities by limiting the will of the majority. Following surveys would make the Fourth Amendment too shackled to the preferences of the majority. Moreover, it would strike many as illegitimate because the Constitution is supposed to transcend the will of the majority at any particular moment in time.

Second, and most compellingly, surveys are deficient to measure reasonable expectations of privacy because people's behavior often fails to match their stated preferences for privacy.[55] Professors Alessandro Acquisti and Jens Grossklags observe that "recent surveys, anecdotal evidence, and experiments have highlighted an apparent dichotomy between privacy attitudes and actual behavior. . . . [I]ndividuals are willing to trade privacy for convenience or to bargain the release of personal information in exchange for relatively small rewards."[56] It is easy

---

[52] Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 Duke L.J. 727, 732 (1993).

[53] *Id.* at 774.

[54] *See, e.g.*, Bloom, *supra* note 48, at 46; Slobogin & Schumacher, *supra* note 52, at 774.

[55] *See* Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality: A Survey*, *in* Privacy and Technologies of Identity: A Cross-Disciplinary Conversation 15, 16 (Katherine J. Strandburg & Daniela Stan Raicu eds., 2006).

[56] *Id.*

to state in a survey that one really values privacy, but what people truly value in practice is revealed by their behavior.[57]

Although behavioral data appears to be more accurate than surveys, behavioral data also suffers from significant shortcomings in measuring people's preferences. People often fail to understand the implications of their behavior on their privacy. Information is often gathered in pieces, here and there, and with each particular piece, a person might not perceive a substantial invasion. When the information is combined, however, people may be surprised at how much about their personalities, interests, and intellectual pursuits is revealed. I have referred to this phenomenon as the "aggregation effect."[58]

Both survey and behavioral data are also deficient because they often reflect what people think and do without full awareness of the consequences. Consider, for example, whether there is a reasonable expectation of privacy in trash. In 1998 in *California v. Greenwood*, the Supreme Court held that there was no reasonable expectation of privacy in garbage left in bags on the curb.[59] In Professors Slobogin and Schumacher's survey, people provided with examples of government searches rated a search of trash to be in the middle of the pack as to its intrusiveness.[60] They rated a dog sniff of luggage to be more intrusive.[61] Their ratings might not have been the same, however, if more about the nature of the searches were pointed out to them. A dog sniff can divulge only limited information about the contents of one's luggage, which often does not contain particularly revealing things. One's trash, however, can contain very revealing information, such as personal writings and even genetic data from hair samples or the like. In further empirical research, Professor Slobogin notes that people rate searches of their credit card records, pharmacy records, and bank records as very intrusive.[62] Yet all of this information is revealed in trash, where financial records and empty medication bottles are routinely discarded. People's stated preferences and behavior might be quite different if these facts were brought to their attention.

Thus, it is very difficult to measure society's expectations of privacy accurately. Even if a metric could be devised to present a precise pic-

---

[57] *Id.*

[58] Daniel J. Solove, Understanding Privacy 118–19 (2008).

[59] 486 U.S. at 40.

[60] Slobogin & Schumacher, *supra* note 52, at 739–41.

[61] *Id.*

[62] Christopher Slobogin, Privacy at Risk: The New Government Surveillance and the Fourth Amendment 184 (2007).

ture of what people expected to be private when fully informed, the reasonable expectation of privacy test would still be flawed for several reasons. First, technology would gradually erode what people expected to be private, and this erosion would allow the government to engage in ever more invasive searches. Second, expectations of privacy depend in part on the law, so judicial decisions about reasonable expectations of privacy would have a bootstrapping effect. If the Supreme Court said there was or was not a reasonable expectation of privacy in something, then that pronouncement would affect people's future expectations.[63] Third, the government could condition the populace into expecting less privacy. For example, as Professor Anthony Amsterdam has observed, the government could diminish expectations of privacy by announcing on television each night that we could all be subject to electronic surveillance.[64]

Looking at expectations is the wrong inquiry. The law should protect certain information regardless of whether people expect it to be private or not. What matters is what people desire. We look to the law not just to preserve the status quo, but to change it and to shape society into what we want it to be.

Consider people's expectations in privacy of the mail. For much of history, people did not expect privacy in their letters.[65] From colonial times, through the American Revolution and long into the nineteenth century, there was widespread fear that one's letters were being illicitly opened by those who delivered them.[66] Many laws were passed to buttress protection of the mail.[67] People wanted their letters to be protected as private even when they were not particularly private. According to David Seipp, "[n]ineteenth century public opinion regarded the 'sanctity of the mails' as absolute in the same way it esteemed the invio-

---

[63] *See, e.g.*, Michael Abramowicz, *Constitutional Circularity*, 49 UCLA L. Rev. 1, 60–61 (2001) ("Fourth Amendment doctrine . . . is circular, for someone can have a reasonable expectation of privacy in an area if and only if the Court has held that a search in that area would be unreasonable."); Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 Sup. Ct. Rev. 173, 188 (arguing that whether a person has a reasonable expectation of privacy is "circular" because "such an expectation will depend on what the legal rule is"); Robert C. Post, *Three Concepts of Privacy*, 89 Geo. L.J. 2087, 2094 (2001) ("[J]udicial interpretations of 'reasonable expectations' will affect the actions of law enforcement agencies, which in turn will affect the actual social norms that define privacy.").

[64] *See* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 Minn. L. Rev. 349, 384 (1974).

[65] Solove, The Digital Person, *supra* note 4, at 225.

[66] *Id.*

[67] *See id.*

lability of the home."[68] It was society's *desire* that letters be private—not its expectation—that sparked the law to make it so.

But even measuring desires fails to address an overarching problem: we might want to regulate government information gathering even when it does not violate privacy. The problem with a doctrinal test based on privacy is that it ensnares courts and commentators into a debate over the meaning of privacy and takes the focus away from the full range of problems the Fourth Amendment needs to address. Practical consequences are ignored in an analytic approach that is nearly blind to the results.

Imagine you had a choice between which of the following two government information gathering activities should receive Fourth Amendment protection: (1) government agents at the border squeeze the outside of people's luggage without opening it; or (2) the government launches a new satellite and surveillance camera system that can track and record all citizens' activities in public throughout their lifetimes.

The first activity is regulated by the Fourth Amendment.[69] In 2000, in *Bond v. United States*, the U.S. Supreme Court considered a search in which a border patrol agent squeezed a bus passenger's canvas bag and noticed a brick-like object that turned out to be methamphetamine.[70] The Court held that the search violated the Fourth Amendment because bus passengers do not expect their bags to be squeezed.[71]

The second activity, however, likely would not be regulated by the Fourth Amendment. The Supreme Court has concluded that people lack a reasonable expectation of privacy in being observed in public. In 1983, in *United States v. Knotts*, the Court held that people lack a reasonable expectation of privacy when the government tracks their movements outside their home.[72] Similarly, in 1986, in *California v. Ciraolo*,

---

[68] Note, *The Right to Privacy in Nineteenth Century America*, 94 HARV. L. REV. 1892, 1899 (1981).

[69] *See* Bond v. United States, 529 U.S. 334, 336 (2000).

[70] *Id.*

[71] *Id.* at 338–39 ("A bus passenger clearly expects that his bag may be handled. He does not expect that other passengers or bus employees will, as a matter of course, feel the bag in an exploratory manner.").

[72] 460 U.S. 276, 282–85 (1983) ("Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.").

the Court held that while in public, people lack a reasonable expectation of privacy from visual observation from above.[73]

Massive and extensive government surveillance in public raises many concerns for freedom and democracy. Surveillance gives extensive power to the watchers. The government could develop a repository of information about citizens and then use any instances of infraction as a pretext to attack people for things they say or for their political beliefs and activities. The government could also use any embarrassing information gleaned from surveillance to blackmail people. Government officials could leak such information either through carelessness or to intentionally retaliate against a person or smear them. Surveillance could chill speech, association, and other forms of dissent.

Even if such systematic government surveillance should be permitted, it deserves at least some degree of oversight and regulation. But under current Fourth Amendment law, a little squeeze of a bag on a bus is fully regulated whereas systematic surveillance is not. These results are misguided and incoherent. The focus should not be on which government activities invade privacy; it should be on which government activities should be regulated.

I therefore join those who contend that the reasonable expectation of privacy test should be abandoned. Among those who have made this contention, Professor William Stuntz argues that "[b]y focusing on privacy, Fourth Amendment law has largely abandoned the due process cases' concern with coercion and violence."[74] Professor Raymond Ku contends that the Fourth Amendment should be understood as protecting against excessive government power and "preserving the people's authority over government."[75] Professor Jed Rubenfeld states that the "Fourth Amendment does not guarantee a right of privacy. It guarantees—if its actual words mean anything—a right of *security*."[76]

---

[73] 476 U.S. 207, 215 (1986) ("In an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet.").

[74] William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 Yale L.J. 393, 446 (1995).

[75] Raymond Shi Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 Minn. L. Rev. 1325, 1326 (2002).

[76] Jed Rubenfeld, *The End of Privacy*, 61 Stan. L. Rev. 101, 104 (2008); *see also* Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 Wake Forest L. Rev. 307, 309 (1998) ("[T]he Fourth Amendment's protections act negatively—to exclude the government from unreasonably searching or seizing one's person, house, papers, and effects. Without the ability to exclude, a person has no security.").

Scholars and jurists propose various candidates for the central thing the Fourth Amendment protects against—physical trespasses, invasions of privacy, government power, excessive coercion, and general warrants.[77] But the Fourth Amendment need not be boiled down to addressing a singular core problem. As Professor William Cuddihy has argued in his comprehensive history of the origins of the Fourth Amendment, "[t]he history that preceded the Fourth Amendment . . . reveals a depth and complexity that transcend language. . . . The [A]mendment expressed not a single idea but a family of ideas whose identity and dimensions developed in historical context."[78]

We should move past the endless attempts to find the core meaning of the Fourth Amendment or to identify a singular type of problem to trigger its protections. In the next Part, I propose a way forward.

II. A Pragmatic Approach

Sizing up our current situation, the problem is that the Fourth Amendment has long been asked to do something it is not particularly well-designed to do—serve as a regulatory system for government information gathering in a world of pervasive data and burgeoning technology. We are using a one-sentence pronouncement of general principles to regulate a wide array of government information gathering activities. The Constitution is not a statutory code. It often does not speak in great detail, especially in the Bill of Rights. Instead, it states broad principles and defines the limits and basic contours of government power. It guides courts in evaluating which statutes are proper and which are invalid.

Currently, the Fourth Amendment remains the primary regime for regulating government information gathering. Certain forms of government information gathering (such as wiretapping and bugging, among other things) are regulated by statute, but most are regulated by the Fourth Amendment or nothing at all.

---

[77] *See, e.g.*, Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 Mich. L. Rev. 547, 551 (1999) ("[T]he historical concerns [underpinning the Fourth Amendment] were almost exclusively about the need to ban house searches under general warrants."); Tracey Maclin, *When the Cure for the Fourth Amendment Is Worse Than the Disease*, 68 S. Cal. L. Rev. 1, 9 (1994) ("Everyone, including [Professor Akhil Reed] Amar, agrees that the Framers opposed general warrants."); Sundby, *supra* note 38, at 1777 (arguing the Fourth Amendment involves the "'trust' between the government and the citizenry").

[78] William J. Cuddihy, The Fourth Amendment: Origins and Original Meaning 770 (2009).

A pragmatic approach to the Fourth Amendment recognizes this reality. We should sweep aside all the tests for Fourth Amendment coverage, stop all the game-playing, and start focusing on the hard practical issue of how best to regulate government information gathering. The Fourth Amendment should cover government information gathering comprehensively rather than haphazardly. A simple tenet of pragmatism is that when there is a problem, one should try to understand it and then solve it.[79]

The Coverage Question should thus be an easy one. The Fourth Amendment should regulate government information gathering whenever it causes problems of reasonable significance. Government information gathering often poses significant problems affecting freedom and democracy. Government information gathering activities can invade privacy and inhibit freedom of speech and association. They make people more frightened to explore ideas. They allow the government to amass enormous quantities of citizens' personal information, which gives the government a vast amount of unchecked power and discretion. They can lead to abuses by law enforcement officials. The Fourth Amendment should provide coverage whenever any of these problems might occur—or when any other problem of reasonable significance might occur. These problems are of a constitutional magnitude, for they are fundamental to the scope of the government's power, the government's relationship to the people, and the people's ability to exercise autonomy, engage in free speech, communicate with others, associate in groups, participate in political activities, pursue self-development, and formulate their own ideas, beliefs, and values.

The harder question is the Procedure Question: how are particular government information gathering activities to be regulated? Unfortunately, the Coverage Question has often diverted attention away from tackling the more difficult Procedure Question. This is a cop out.

The way forward is to face the Procedure Question rather than try to avoid it. If the Fourth Amendment lacks a sufficiently broad array of

---

[79] 12 John Dewey, *Logic: The Theory of Inquiry*, *in* The Later Works 1, 110–13 (Jo Ann Boydston ed., 1986).

> The point made can be most readily appreciated in connection with scientific reasoning. A hypothesis, once suggested and entertained, is developed in relation to other conceptual structures until it receives a form in which it can instigate and direct an experiment that will disclose precisely those conditions which have the maximum possible force in determining whether the hypothesis should be accepted or rejected.

Id.

regulatory options, then more should be crafted. Problematic government information gathering activities should not be left completely unregulated because of some crabbed theory of the Fourth Amendment's scope.

A. *Oversight and Regulation*

We should face the reality that the Fourth Amendment has become the central regulatory system for government information gathering. In many ways, it is being asked to function like a statutory regime because there is a big void to fill. Although it works best as a guide for evaluating statutes, it must set forth rules when there are no statutes in place. Fourth Amendment coverage should not be carved up in arbitrary ways so as to avoid performing this role.

A pragmatic approach would focus on practical consequences and move past analytical games. We should begin by looking at the problems created by government information gathering activities. The scope of Fourth Amendment protection should be determined by asking whether a particular government information gathering activity causes problems of reasonable significance.

Under this approach, the Fourth Amendment would likely apply to a very broad range of government information gathering activities. The tougher issues emerge with the Procedure Question: if the Fourth Amendment applies, how should a particular government information gathering activity be regulated? The Fourth Amendment should not demand a one-size-fits-all rule requiring a warrant supported by probable cause.[80] Various forms of oversight and regulation can be costly and can make investigatory activities too inefficient to be worthwhile. We must assess the value of the information gathering activity and consider it in light of the importance of ameliorating the problems it causes. The analysis should address questions such as: Is this information gathering activity one that government should perform frequently? Rarely? Early on in an investigation? Only as a last resort? In particular cases involving only those suspected of crimes? En masse to the entire population?

---

[80] Fabio Arcila, *The Death of Suspicion*, 51 Wm. & Mary L. Rev. 1275, 1341 (2010) ("A large problem with current Fourth Amendment law is that it veers wildly between two opposing poles—the strict application of the presumptive warrant or suspicion requirements on one hand, and effectively unconstrained balancing through a totality-of-the-circumstances approach in the other.").

Even the exclusionary rule is not sacrosanct under such an approach. The approach to what enforcement mechanism should be required for Fourth Amendment violations should be determined by focusing on the practical consequences.

In most cases, a particular form of oversight and regulation can be devised that will allow the government to engage in information gathering but will minimize many problems created by such gathering. Consider, for example, the collection of genetic information. Suppose the government wants to obtain a person's DNA. The police follow the person around, waiting for her to discard an item from which they can obtain her genetic information. Under current doctrine, will the Fourth Amendment provide protection in this instance? The answer is likely no.[81] Although the U.S. Supreme Court has not yet addressed the issue, courts have thus far concluded that people lack a reasonable expectation of privacy in such situations, relying primarily on the 1988 Supreme Court case of *California v. Greenwood* and analogizing abandoned objects containing DNA to abandoned trash.[82] In 2006, in *Commonwealth v. Ewing*, the Massachusetts Appeals Court concluded that a person lacked a reasonable expectation of privacy in a discarded cigarette, which was subsequently used to obtain his DNA, because he "voluntarily abandoned [the cigarette] as trash."[83] Likewise, in 2007, in *State v. Athan*, the Washington Supreme Court considered a situation in which the police had tricked a defendant by pretending to be attorneys involved in a class action and asking whether the defendant wanted to be included in the class.[84] The defendant returned a reply envelope, and the police obtained his DNA from the saliva he used to seal it.[85] The Washington Supreme Court held that "[p]olice may surreptitiously follow a suspect to collect DNA, fingerprints, footprints, or other possibly incriminating evidence, without violating that suspect's privacy."[86]

The reasonable expectation of privacy test bogs us down in an analytical game, but the crucial questions are lost in the shuffle. Should the government be able to gather everyone's genetic information without any oversight? Should it be able to collect samples without any suspi-

---

[81] *See* Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 Nw. U. L. Rev. 857, 862 (2006) ("In cases involving 'abandoned DNA,' however, the police have been able to retrieve the most detailed genetic information, without being subject to the criminal procedure rules that normally apply to searches and seizures.").

[82] *See* California v. Greenwood, 486 U.S. 35, 50 (1988).

[83] 854 N.E.2d 993, 1001 (Mass. App. Ct. 2006).

[84] 158 P.3d 27, 31 (Wash. 2007).

[85] *Id.* at 32.

[86] *Id.* at 37.

cion at all? Should it be able to use the samples however it desires and keep them for as long as it wants? Should it be able to do this systematically for millions of people without any limitation? To what degree should the government be able to use trickery and deception in order to obtain DNA information?

Genetic information can reveal quite a lot about a person's medical past and future, as well as information about her family members.[87] Some oversight and limitation of the collection and use of this information might prevent abuses and ensure that DNA is collected only to investigate people suspected of criminal activity. Making the government seek judicial authorization—even a warrant supported by probable cause—does not prevent the police from obtaining DNA through abandoned items.

Another example is the application of the third party doctrine beyond the context of phone and bank records. In what is known as "cloud computing," users access software via the Internet and, in some cases, store their documents, videos, and photos remotely. Google Docs, for example, allows people to upload word processing documents, spreadsheets, and other files to Google's servers, a function that is useful for backing up data or editing documents jointly with others. Because these documents are no longer stored on people's home computers but with a third party, they might fall outside of Fourth Amendment protection. Some contend that the third party doctrine applies only to a limited class of data, not to the content of all documents and communications.[88] Others view the doctrine more broadly, as applying to all personal information possessed by third parties.[89]

---

[87] *See, e.g.*, Michelle Hibbert, *DNA Databanks: Law Enforcement's Greatest Surveillance Tool?*, 34 Wake Forest L. Rev. 767, 782 (1999) (noting that a DNA profile "not only reveal[s] extensive genetic information about the individual whose 'genetic fingerprint' is on file, but also about his or her close relatives"); Sonia M. Suter, *Disentangling Privacy from Property: Toward a Deeper Understanding of Genetic Privacy*, 72 Geo. Wash. L. Rev. 737, 739 (2004) (explaining that DNA influences our "temperament, health, capacities, and physical appearance").

[88] *See* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 Geo. Wash. L. Rev. 1557, 1581 (2004) (noting that *Smith v. Maryland*, 442 U.S. 735 (1979) distinguished *Katz v. United States*, 389 U.S. 347 (1967) based on "the limited information that can be gleaned from a phone number, contrasting it with what may be revealed from a telephone conversation").

[89] *See* Computer Crime & Intellectual Prop. Section Criminal Div., Dep't of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 6–10 (2009), *available at* http://www.justice.gov/criminal/cybercrime/ssmanual/ssmanual2009.pdf.

The debate is difficult to resolve because the Supreme Court's decisions are incoherent.[90] In 1979, in *Smith v. Maryland*, the Court set forth two rationales: (1) the information was merely phone numbers and did not involve "the contents of communications," and (2) people "know that they must convey numerical information to the phone company," and thus they cannot "harbor any general expectation that the numbers they dial will remain secret."[91] Does this mean that the third party doctrine only applies when the information is not as sensitive as the content of communications? Or does it apply whenever records are in the hands of third parties? *United States v. Miller*, decided by the Court in 1976, a few years before *Smith*, applied the third party doctrine to bank records and suggested a broader interpretation of the third party doctrine.[92] But would the third party doctrine apply to medical records? After all, people expose their medical conditions to their doctors. Would the Supreme Court really hold that people lack an expectation of privacy in their medical data because they convey that information to their physicians? This result would strike many as absurd.

This debate can be sidestepped entirely with the pragmatic approach I am proposing. Under such an approach, there is a strong argument that government access to records held by third parties should be subject to oversight and regulation. It is increasingly the case that much of what we do, buy, and read generates records maintained by third parties. Regulation and oversight should not turn on the happenstance of where such records are located, and changing technology that increasingly locates them outside people's homes should not suddenly cause them to drop out of the regulatory regime.

We should not be debating whether people expect privacy in records held by third parties. Such a debate misses the more fundamental questions: Should government gathering of records held by third parties be regulated and subjected to oversight? If so, what kind of regulation and oversight would best balance law enforcement goals with protection against harm?

Interestingly, Professor Orin Kerr, who has provided the most robust defense of the third party doctrine, focuses his arguments on practical considerations about how the application of the Fourth Amendment will affect law enforcement investigations—not on the fact that

---

[90] *See, e.g.*, *Smith*, 442 U.S. at 741; United States v. Miller, 425 U.S. 435, 442 (1976).

[91] *See* 442 U.S. at 741, 743 (italics omitted); *supra* notes 40–41 and accompanying text.

[92] *Miller*, 425 U.S. at 442 ("All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.").

people lack privacy in their records.[93] Kerr points to statutory and other regulations for records held by third parties that he believes provide a better system of regulation, "a middle ground not possible under the Fourth Amendment."[94]

Kerr finds it best to place records held by third parties outside of the Fourth Amendment's scope because he finds the Amendment's regulatory rules to be deficient.[95] But there are many types of records maintained by third parties that are not protected at all by statute or by any of the alternative regulatory mechanisms he discusses.[96]

Instead of excluding something from Fourth Amendment coverage just because of problems with Fourth Amendment rules, the solution is to improve those rules rather than provide no protection. Government access to records held by third parties should be covered by the Fourth Amendment. If the legislature seeks to regulate these records by statute, the courts should evaluate the efficacy of that statute in terms of how well it balances the problems and benefits of government access. By placing such activities outside the Fourth Amendment's coverage, the Supreme Court has adopted the rather ludicrous position that people lack privacy in records held by third parties. Why keep playing this game? Why not just face the hard issues and figure out how best to regulate government access to records in the hands of third parties? This debate should sound not in privacy, but in the practical consequences—the benefits and costs of regulation and oversight. This is the debate we should be having over the Fourth Amendment, not a debate about its applicability.

B. A *Response to Potential Objections*

There are several potential objections to the pragmatic approach I am proposing. First, in the "inconsistency objection," one might contend that my approach would lead to too much inconsistency in the law. Second, in the "textualist objection," one might contend that the

---

[93] *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 597 (2009).

[94] *See id.*

[95] *See id.* ("In many (but not all) of these cases, the statutory privacy laws provide less protection than would the analogous Fourth Amendment standard of a probable cause warrant. But that is a good thing rather than a bad one. . . . These intermediate standards deter wrongful abuse while permitting legitimate investigations.").

[96] *See* SOLOVE, THE DIGITAL PERSON, *supra* note 4, at 202–09. For example, "[r]ecords held by bookstores, department stores, restaurants, clubs, gyms, employers, and other companies are not protected [by statute from government access]." *Id.* at 208.

pragmatic approach is too indeterminate because it is not sufficiently tethered to the actual text of the Fourth Amendment. Third, in the "usurpation objection," one might argue that the pragmatic approach encroaches too much upon the province of the legislature.

1. The Inconsistency Objection

Professor Kerr argues that focusing on policy would be unworkable because "lower courts cannot administer it consistently."[97] He notes that the Supreme Court only resolves a fraction of the Fourth Amendment cases decided per year: "[T]he Supreme Court's decisions cover only a tiny sliver of fact patterns common in police investigations."[98] He believes that looking directly at policy is too fact-specific because "it asks courts to assess whether a particular set of practices require regulation, inviting a balancing of interests over the range of those facts that fall within the defined practice."[99] This leads to instability in the law.[100]

Kerr identifies bona fide problems, but they are problems endemic to many areas of law. Indeed, the reasonable expectation of privacy test also leads to many ambiguities. As I discussed earlier, there are many open questions with regard to the scope of the third party doctrine. Courts will always struggle when determining what situations are analogous to previous decisions.

Clear and consistent rules could readily be established by looking to policy. Moreover, my approach would determine the applicability of the Fourth Amendment not based on balancing, but based on whether there are problems of reasonable significance caused by government information gathering. If there is a problem, then the Fourth Amendment would regulate. Courts would determine what degree of oversight and regulation is best suited to ameliorate the problem. My approach differs from the reasonable expectation of privacy test in that it recognizes *all* of the problems caused by government information gathering, not just privacy problems.

For the initial Coverage Question, my approach would provide much clearer results than the reasonable expectation of privacy test. Most government information gathering activities would be covered. For the Procedure Question, courts would, over time, develop a set of

---

[97] Kerr, *supra* note 5, at 536.
[98] *Id.* at 539.
[99] *Id.* at 539–40.
[100] *See id.* at 540.

principles to evaluate legislation as well as specific rules in the absence of legislation. There is no reason why this jurisprudence cannot be clear and coherent.

2. The Textualist Objection

The principal contention under the textualist objection is that the pragmatic approach threatens to turn the Fourth Amendment into a way for courts to impose their own normative aims on society.

But this is what the Fourth Amendment has already become. Very little of modern Fourth Amendment jurisprudence relates to the Amendment's text. The reasonable expectation of privacy test itself does not emerge from the text. Indeed, the Fourth Amendment does not even include the word "privacy." The doctrine has evolved so far beyond the text of the Fourth Amendment—and beyond the text of most of the Constitution—that text should not be determinative.

Moreover, the Fourth Amendment's text is quite broad, speaking of "unreasonable searches," and thus need not be limited to one particular kind of problem. Just as a search can be unreasonable because it violates privacy, it can be unreasonable because it causes other kinds of problems. The Amendment can be read as a broad pronouncement that whenever the government gathers information, it must do so in a way that minimizes potential problems. It also can be read to ensure that the benefits of government information gathering outweigh whatever problems cannot be eliminated. These requirements—that problems caused by searches be minimized with oversight and regulation and that the benefits of searches outweigh the costs—are common sense, and they should constitute the heart of reasonableness under the Fourth Amendment.

3. The Usurpation Objection

The usurpation objection demands a significantly more detailed response. According to this argument, the pragmatic approach would usurp the function of the legislative branch. The judicial branch would effectively get more leeway to craft whatever system of regulation it wants.[101] Even beyond new technologies, some might argue that the

[101] *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 858 (2004). As Professor Kerr argues, "[c]ourts tend to be poorly suited to generate effective rules regulating criminal investigations involving new technologies. In contrast, legislatures possess a significant institutional advantage in this area over courts." *Id.*

rules that govern how the government should use its powers of information gathering should be determined by democratically elected legislatures, not crafted by judges, who are detached from the will of the people and lack the expertise of law enforcement officials.

Although this objection has merit, the reality is that only in limited circumstances have legislatures been active in crafting rules to regulate government information gathering.[102] When the Fourth Amendment was initially applied to government information gathering activities, there was little statutory law to regulate them. Moreover, the government's information gathering activities represent one of the most potent forms of government power—and they can affect our freedom and democracy in profound ways. Because these issues are so fundamental to the basic structure of our society, they are justifiably regulated by the Constitution.

Nevertheless, the Constitution generally speaks in broad pronouncements of principle; it lacks the specificity and detail of statutes. Because the Fourth Amendment generally regulates with warrants supported by probable cause and enforced by the exclusionary rule, some might argue that it lacks the nimbleness and flexibility to regulate all of the varied activities of government information gathering.

The Fourth Amendment need not be interpreted rigidly to require a one-size-fits-all rule for all forms of government information gathering. Although the Fourth Amendment generally requires warrants supported by probable cause, the Supreme Court has crafted numerous exceptions to promote greater flexibility. There are exceptions for exigent circumstances,[103] for temporary stops and frisks of suspicious individuals,[104] and

---

[102] *See* Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 Fordham L. Rev. 747, 768–72 (2005).

> Federal legislation is not easy to pass, and it usually takes a dramatic event to spark interest in creating or updating a law. Congress often only gets involved when there is a major uproar or problem, and unless there is a strong impetus, little new lawmaking occurs. . . . As a result, issues are likely to be addressed with more frequency in the courts than in Congress.

Id. at 771.

[103] *See* Illinois v. Rodriguez, 497 U.S. 177, 186 (1990) (holding that the Fourth Amendment is not violated when police officers "enter [a home] without a warrant because they reasonably (though erroneously) believe that they are in pursuit of a violent felon who is about to escape").

[104] *See* Terry v. Ohio, 392 U.S. 1, 30–31 (1968).

> [W]here a police officer observes unusual conduct which leads him reasonably to conclude in light of his experience that criminal activity may be afoot and that the persons with whom he is dealing may be armed and presently

for checkpoints,[105] among many others. The Fourth Amendment has already been interpreted to have a fair degree of flexibility, and there is no reason why it cannot be interpreted to be even more flexible if need be.

It is true, however, that courts crafting rules under the Fourth Amendment will likely not have the same range in palate as a legislature would have. Nothing in my approach prevents a legislature from crafting a rule that diverges from any rule a court might create—so long as that rule satisfies the minimum requirements of the Fourth Amendment.

A related point under the usurpation argument is that a very broad Fourth Amendment scope would deter legislatures from enacting laws to regulate law enforcement. If the Fourth Amendment allows courts to lord over criminal procedure, then legislatures might feel they have hardly any room to create their own rules.

This concern would be significant if courts were to impose their own set of rules under the Fourth Amendment and refuse to accept any alternative rules that legislatures might pass. The Fourth Amendment states only basic principles. Specific rules would come from legislatures, and they would be reviewed by the courts to ensure they satisfied the basic principles of the Fourth Amendment. Only in the absence of legislative rules should courts create their own specific rules. Indeed, as a general rule, whenever there is a legislative rule governing a particular government information gathering activity, courts should merely evaluate it as to whether it meets the basic principles of the Fourth Amendment, not as to whether it is the ideal policy choice.

The pragmatic approach I am proposing expands the scope of Fourth Amendment coverage, but there is still sufficient space for legislatures to create rules to regulate government information gathering.

> dangerous . . . he is entitled for the protection of himself and others in the area to conduct a carefully limited search of the outer clothing of such persons in an attempt to discover weapons which might be used to assault him.

Id. at 30.

[105] *See* Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990).

> [T]he balance of the State's interest in preventing drunken driving, the extent to which this system can reasonably be said to advance that interest, and the degree of intrusion upon individual motorists who are briefly stopped, weighs in favor of the state program. We therefore hold that it is consistent with the Fourth Amendment.

Id.

Conclusion

Fourth Amendment law is in a malaise. It is the primary body of regulation for government information gathering, yet it applies in a patchwork fashion. The problems stem from the reasonable expectation of privacy test, which focuses the debate over the scope of Fourth Amendment protection on the wrong issue—whether privacy is invaded. Courts get bogged down in attempting to elucidate the meaning of "privacy" and fail to look at the full range of problems caused by government information gathering. It is time to move past the reasonable expectation of privacy test and adopt a more pragmatic approach to the Fourth Amendment.