REFORMING FOURTH AMENDMENT PRIVACY DOCTRINE

JIM HARPER*

TABLE OF CONTENTS

INTRODUCTION

As courts have adapted the Fourth Amendment[1] to modern life, a doctrine has grown up around it that is unnecessarily complex and ultimately unworkable. This has deprived the Fourth Amendment of strength and—especially since the attacks of September 11, 2001—allowed Americans' Fourth Amendment rights to recede.

* Director of Information Policy Studies, The Cato Institute. B.A. 1990, *University of California, Santa Barbara*; J.D. 1994, *Hastings College of the Law.*

1. U.S. CONST. amend. IV.

Surveillance within the United States has increased since terrorism captured the national consciousness in late 2001. A wide variety of government programs, nominally aimed at terrorists, have begun or increased the collection of information about the communications, finances, movements, and activities of all Americans.

What should be done to restore Americans' freedom—and their sense of freedom—so that a vibrant, open polity on the North American continent is assured? Many things, of course, but a very important one is to reinvigorate the Fourth Amendment by reforming Fourth Amendment privacy doctrine.

Since 1967, the Supreme Court and lower courts have relied too heavily on an unreliable test that arose from the leading Fourth Amendment case, *Katz v. United States*.[2] Distracted by Justice Harlan's concurrence in the case and befuddled by the concept of "privacy," courts have ignored the simple rule of the actual holding in *Katz* and conditioned Fourth Amendment rights on surmises about privacy "expectations."

Privacy is a real thing that need not be a matter of conjecture. The *Katz* Court held that personal information was protected by the Fourth Amendment because, as a factual matter, the defendant had kept it private.[3] Installing a wiretap to overcome Katz's use of law and physics to conceal information was unreasonable without a warrant.[4] The Court did not base its holding on open-ended "expectations" or "reasonableness," as Justice Harlan's concurrence suggested, but on the affirmative steps Katz took to conceal that information.

Though the Court's escape from the *Olmstead v. United States*[5] decision in *Katz* was welcome,[6] the test Justice Harlan suggested in dictum about privacy "expectations" is impossible to administer, and it creates a one-way ratchet against privacy and Fourth Amendment protection.[7] Its weakness is clearly demonstrated by the leading decision on communications privacy, the regrettable *Smith v. Maryland*.[8]

2. 389 U.S. 347 (1967).
3. *Id.* at 353.
4. *See id.* at 358 (concluding that the need for a "neutral predetermination of the *scope* of a search" does not disappear when transferred to the setting of a telephone booth).
5. 277 U.S. 438 (1928), *overruled by Katz*, 389 U.S. 347.
6. *See Katz*, 389 U.S. at 353 (announcing that the trespass doctrine in cases such as *Olmstead* was no longer controlling).
7. *See id.* at 361 (Harlan, J., concurring) (framing the emerging rule as a two-part test requiring a subjective and objective expectation of privacy).
8. *See* 442 U.S. 735 (1979) (holding that individuals have no right to privacy in the telephone numbers they dial).

Unfortunately, the circularity of the "reasonable expectation of privacy" test is not broken by importing First Amendment considerations. Rather, it is solved by abandoning that test and treating privacy as a factual question, as the Court's majority did in *Katz* and in its 2001 decision, *Kyllo v. United States*.[9] If an individual has secured the privacy of particular information, the Fourth Amendment focuses on the reasonableness of the government's actions in undoing that privacy, not on the reasonableness of the individual's expectations. Once courts recognize this, and end the "third party doctrine," the Fourth Amendment will be back on the strong footing it deserves.

The Court's Unsteady Escape From Olmstead

Katz is the lodestar Fourth Amendment ruling that rescued electronic search-and-seizure law from the retrograde *Olmstead* decision. In *Olmstead*, warrantless wiretaps of bootleggers' homes and offices had secured the evidence needed to convict them, and the Court rejected their constitutional challenge.[10] Writing for the Court, Chief Justice Taft fixed on the material things listed in the Fourth Amendment's search and seizure clause—"their persons, houses, papers, and effects."[11] Wiretapping had not affected any of the defendants' physical possessions, he found, so it had not affected their Fourth Amendment rights.[12] This gave short shrift to the real object of the Fourth Amendment's protection, of course: "the right of *the people* to be secure . . . ."[13]

In dissent, Justice Brandeis criticized the Court's literalism, and honed in on the Founders' libertarian individualism:

> 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,

9. *See* 533 U.S. 27 (2001) (finding search unconstitutional where police used thermal imaging technology to gather evidence about the temperature inside defendant's home).

10. *See* 277 U.S. at 466 ("We think, therefore, that the wire tapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment.").

11. *Id.* at 457, 464.

12. *Id.* at 464.

13. U.S. CONST. amend. IV (emphasis added).

> the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.[14]

Though not the first,[15] Brandeis's pronouncement remains a prominent and lasting tie in Supreme Court case law between the Fourth Amendment and privacy. The amendment itself, of course, makes no specific mention of this interest.

Before rising to the Supreme Court, Brandeis had co-authored the seminal Harvard Law Review article, *The Right to Privacy*.[16] His link as a jurist between the Fourth Amendment and privacy was welcome, but he did not bind them as tightly as he might have. Referring to privacy as "the right to be let alone,"[17] for example, Justice Brandeis did not describe the human interest most threatened by the government's wiretapping in the case.

Olmstead and his fellow booze merchants had not had their solitude undone by the warrantless wiretaps. They were not restrained, interrupted, or interfered with by the wiretaps later used to convict them. Surveillance of them had not affected their sense or—for the most part—the reality of being "let alone." Brandeis correctly believed that investigators had violated the privacy of Olmstead and his cohorts, but his writing left unclear what he meant by "privacy."

The Katz *Court: Privacy! But . . . What is That?*

Justice Brandeis's marriage of the Fourth Amendment and privacy was vindicated in *Katz*, which reversed *Olmstead* in 1967.[18] FBI agents had placed a recording device on the outside of a public telephone booth to eavesdrop on the conversations of an individual they suspected of transmitting wagering information.[19] This violated defendant Katz's Fourth Amendment rights, the Court held, reversing his conviction.[20] Justice Stewart's majority opinion embraced and distilled Brandeis's importuning in *Olmstead*, using similarly lasting words:

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or

14. *Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting).
15. *See, e.g.*, Boyd v. United States, 116 U.S. 616, 622 (1886) (determining that compulsory production of a person's private papers to establish a criminal charge against that person is within the scope of the Fourth Amendment).
16. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
17. *Olmstead*, 277 U.S. at 478.
18. 389 U.S. 347 (1967).
19. *Id.* at 348.
20. *Id.* at 359.

> 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.[21]

The Court established that the Fourth Amendment protects individual privacy but, like Justice Brandeis, it did not clearly delineate what that interest is. The Court did sketch a rough outline of the right, however. The Fourth Amendment does not protect a "general constitutional 'right to privacy,'"[22] but it does protect what a person "seeks to preserve as private."[23]

To invoke this protection, one need not act in total secrecy. Katz made his calls from within a public telephone booth constructed partly of glass. Against the government's claim that he had no privacy there, the Court pointed out that glass shields sounds even while it reveals visual information: "[W]hat [Katz] sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen."[24]

By shielding the sound of his voice from the general public, Katz had shielded the sound of his voice from the government, preserving his conversation as private. It did not matter that he had revealed the appearance of his body, the phone is his hand, and his moving mouth. Though undoubtedly free to collect images, investigators could not reasonably (and thus constitutionally) access the sounds of his voice with a wiretap unless they had gotten the special permission of a warrant.[25]

The majority decision in *Katz* treated the privacy interest embodied in the Fourth Amendment as a rule about control of information (which is how Brandeis had meant it in *Olmstead*). The Fourth Amendment's search and seizure clause means that people can control personal information the same way against the government as they do against society as a whole. As a factual matter, Katz had concealed the sound of his voice from the general public, so he had concealed it from the government as well.

21. *Id.* at 351 (citations omitted).
22. *Id.* at 350.
23. *Id.* at 351.
24. *Id.* at 352.
25. *Id.* at 358–59.

Harlan Amends the Katz *Rule, Badly*

Alas, this simple rule was scrambled by a well-meaning concurrence. Justice Harlan described the Court's opinion as flowing from a two-part test:

> My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable."[26]

This was unfortunate dictum. It reversed the Fourth Amendment's focus from the reasonableness of government action (taking private ordering as a given) to the reasonableness of the interests the amendment was meant to protect.

More importantly for judicial administration, it converted a factual question—had the defendant barred others from access to the information?—into a murky two-part analysis with a quasi-subjective part and a quasi-objective part. It is an analysis that courts have mangled ever since. And for good reason: It is almost impossible to administer.

Take "exhibit[ing] an actual (subjective) expectation of privacy."[27] People keep information about themselves private all the time without "exhibiting" that interest in any perceptible way—indeed, without any subjective consideration at all.

Families obscure their bathing behind the walls of their homes, for example, without contemplating that their walls provide them that privacy. Homes are walled for a variety of reasons, of course, including privacy, security, temperature control, and light control. One need not consider these things—much less "exhibit" anything—to have a legitimate, actual interest in them.

Likewise, people maintain privacy in their phone conversations by the simple act of using the phone. The earpiece directs sounds at low volume immediately into the caller's ear, maintaining the privacy of both sides of the conversation (in varying degrees) while preserving the solitude of others nearby.[28] Callers and their neighbors almost never consider these welcome design features, or "exhibit" their desire to maintain privacy or quiet. A phone's handset provides these things all the same.

---

26. *Id.* at 361 (Harlan, J., concurring).
27. *Id.*
28. *See id.* at 352 (majority opinion) (articulating that a person using a telephone booth "is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world").

Our world is built for ornate combinations of privacy and disclosure that are almost always customary, habitual, or subconscious. They are rarely explicit, "exhibited," or a subject of a conscious "expectation." This does not diminish the importance of privacy or counsel against enforcing the constitutional right that protects it.

Constitutional law does not require people to "exhibit" expectations about other constitutionally protected interests. Take life, for example. People exhibit interests very much in tension with long and healthy lives when they inhale cigarettes, martinis, and cheeseburgers, but bad health habits create no argument for weakening due process rights in capital cases. An individual's Fourth-Amendment-backed interest in privacy is real whether or not it is exhibited, consciously considered, or expected.

Perhaps one "exhibits" an interest in the relevant dimension of privacy simply by entering a home, by holding a phone to an ear, or by whatever volition conceals information from others. In its best light, the first part of the inquiry Justice Harlan proposed merely restates the majority's holding in *Katz*. If a person has privacy—if the information was not generally available—he or she has "exhibited" an "actual (subjective) expectation of privacy."[29]

The second part of the test has no similar good reading. What, in any given circumstance, does society find reasonable to keep private? It is a question that philosophers would not be able to answer nor sociologists be able to gauge—to say nothing of courts trying to administer people's constitutional rights. The question whether society recognizes as reasonable the privacy of a given unit of information sounds like an objective test, but it is not. There is no objective standard for whether privacy is reasonable.

Take one example. Health and medical information is often kept private. On passage of the Health Insurance Portability and Accountability Act of 1996[30] and during the process of writing the privacy regulations under that law, advocates and the regulation writers intoned about health information being consumers' "most

29. *Id.* at 361 (Harlan, J., concurring).

30. Pub. L. No. 104-191, 110 Stat. 1936 (codified at scattered sections of 18 U.S.C., 26 U.S.C., 29 U.S.C., and 42 U.S.C. (2000)). In point of fact, HIPAA was aimed at privacy, but punted on the meaning of it. Congress asked the Secretary of Health and Human Services to make recommendations about the privacy of individually identifiable health information, and to go ahead and regulate in pursuit of privacy if Congress did not act. *Id.* at tit. 2, pt. C, § 264. Sure enough, Congress did not act. The HIPAA privacy regulations were a product of pure administrative surmise about what privacy is and what serves it.

sensitive information."[31] This is a sound observation, of course—until one observes actual human behavior.

In fact, people often appreciate and benefit from wide disclosure of their medical conditions and treatments. "Get Well Soon" cards exist precisely because people often share highly intimate medical information and enjoy broad acknowledgment of their conditions. Voluntarily made video and text reports of people's open-heart surgeries, cancer treatments, and various other maladies and remedies are easy to find on the Internet.[32]

Health information is some of the most private, except when publicity takes priority. The same is true of information about people's political views and voting behavior, their sexual orientation and activity, their reading, their travels, and so on. People's privacy and publicity interests vary widely and endlessly. They hide information or share it based on culture, habit, custom, upbringing, and experience, making individual privacy or publicity decisions that defy capture. The only consistent explanation is that privacy is a subjective condition that is highly circumstance-specific. It is not susceptible to objective determination.

Unworkable as a true legal test, the second part of the formulation Justice Harlan proposed in *Katz* is simply an invitation for judges to import their personal views and alter the actual rule set down in the case. It replaces the individualistic conception of privacy that Justice Brandeis promoted with a call for generalizations that cannot be reliably administered. Fundamentally, Justice Harlan's concurrence is at odds with the majority holding in the case.

The Katz *Majority Opinion Does Not Support Harlan's Concurrence*

In fairness, the phrasing of the *Katz* majority opinion left ajar the door that Harlan threw open. But the Court did not mean to allow that. Consider the language again: "What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection. . . . But what he seeks to preserve as private . . . may be constitutionally protected."[33] The auxiliary verb "may" in the latter sentence gives it open-endedness. The word can indicate either

31. Department of Health and Human Services, Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,181, 53,182 (Aug. 14, 2002) (to be codified at 45 C.F.R. pts. 160, 164).

32. *See, e.g.*, YouTube.com, Stoughton Toddler Has Successful Open Heart Surgery, http://www.youtube.com/watch?v=RjXarBU5tZo (naming, picturing, and depicting the heart surgery of a Massachusetts boy, with interviews of parents and doctor).

33. Katz v. United States, 389 U.S. 347, 351 (1967) (majority opinion).

permission or possibility, and there are several ways to interpret the sentence. The best of them points toward giving Katz constitutional protection based simply on his good husbandry of information, not on Justice Harlan's further inquiry about his expectations or the reasonableness of them.

If "may" were to indicate permission (i.e., Katz *is allowed* to protect this information), the sentence would be passive, unlike the preceding active sentence that it parallels. It would also beg the question that the Court purports to be answering. Given the parallel sentence structure and the forcefulness of the paragraph, it is unlikely that the Court intended to use "may" in its permissive sense.

The better reading of the case is that "may" indicates possibility—that constitutional protection of Katz's conversations turns on some contingency. But what contingency? The most likely is right there in the sentence: whether or not something is "preserve[d] as private."[34]

The paragraphs following this key sentence discuss the facts that caused the Court to conclude that Katz's phone conversations were constitutionally protected—his presence in a phone booth made of glass, with its useful sound-dampening qualities.[35] Katz sought to preserve the privacy of his phone conversation, and succeeded. With that condition cleared up, the sentence comes to mean, "What he preserved as private is constitutionally protected."

The majority decision did not raise or explore additional conditions controlling whether phone conversations might be protected. This is what Justice Harlan did, alone suggesting the "expectation" and "reasonableness" conditions on Fourth Amendment protection for private information.

This was a disservice to the courts and lawyers later trying to apply the *Katz* decision to new facts. But more importantly it was a disservice to privacy and the Fourth Amendment. Justice Harlan's test established a one-way ratchet against Fourth Amendment protection.

We've Got "Plain View"—Why Not "Plainly Concealed"?

The "plain view" doctrine is a constitutional test so simple that most people do not even realize it is a test. If a thing is visible (or otherwise perceivable) by authorities acting within law and custom, a person cannot make a Fourth Amendment claim against them

34. *Id.*
35. *Id.* at 352.

observing it and acting on the knowledge of it.[36] If a person has not concealed something against others, he or she has not concealed it from the government.

This was stated as common sense in the *Katz* decision—"[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection"[37]—and it is the mirror image of the holding, where concealment against others was concealment against the government. But Harlan's concurrence placed a special impediment on concealment and privacy that has never been proposed for "plain view" or exposure. Somehow "plain view" is a simple factual question but "plain concealment" gets further consideration.

Imagine if there were a "Harlan concurrence" to the plain view doctrine. It might go like this:

> My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person has exhibited an actual (subjective) expectation of exposure and, second, that the expectation be one that society is prepared to recognize as "reasonable."

Using this test, courts might examine whether a person had exhibited the expectation that something of his or hers should be left visible and, if so, whether leaving such things visible was considered "reasonable." There might be instances where something plainly observable to all who pass could not be noted or considered by law enforcement because of "reasonable expectations of privacy." Judges who thought society demanded greater privacy would reverse convictions when someone had left something visible that he or she would not have, in exercise of reasonableness, according to the judge's opinion of society's beliefs.

Of course, there is no such gloss on the plain view doctrine. The question whether something is in plain view is a factual one. So should be the question whether something is concealed. To restate again, in *Katz*, the defendant had obscured his voice from others as a matter of fact. The government's acquisition of his conversation by unusual means without a warrant was unreasonable and violated his Fourth Amendment rights.

Restoring the actual rule of *Katz* would restore symmetry to Fourth Amendment doctrine. It has long been held, sensibly, that one cannot claim privacy or Fourth Amendment protection in something

36. *See, e.g.*, Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971) (outlining the parameters of the plain view doctrine and finding that the seizure of two automobiles parked in the defendant's driveway violated the Fourth Amendment).

37. *Katz*, 389 U.S. at 351.

that one, as a matter of fact, has revealed to the public. There should not be a two-part subjective/"objective" test for the converse rule.

Smith *Shows the Weakness in Harlan's* Katz *Test*

Time and experience have made the weaknesses in Justice Harlan's *Katz* formulation more and more clear. For example, in *Smith v. Maryland*,[38] one of the leading communications privacy cases, the Supreme Court faced the question of whether placement of a pen register[39] on a suspect's phone line without a warrant violated the Fourth Amendment.[40] Applying the test from Harlan's concurrence in *Katz*, the Court asked itself whether Smith had a reasonable expectation of privacy in the phone numbers he had dialed.[41]

The *Smith* Court certainly did not treat the subjective part of the *Katz* test as subjective: "[W]e doubt that people in general entertain any actual expectation of privacy in the numbers they dial."[42] This would not have been surmise, but a fact found at trial had there been faithful application of the test.

For the quasi-objective part of the test, Justice Blackmun walked through many of the influences that would suppress people developing an expectation of privacy in their phone-dialing—and none of the influences that would support it.[43] Given that one-sided analysis, he concluded, "it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret."[44]

Using the word "secret" rather than "private," Justice Blackmun confessed to answering a slightly different question than the one posed, of course. Secrecy and privacy are different grades of information-withholding, with different objects. But so it goes. The "reasonable expectation of privacy" test does not tether courts to solid conceptual footings.

In fact, the numbers one dials when he or she uses a telephone are private. Unless one allows his or her fingers to be observed pressing the buttons, or the tones to be overheard or recorded, only the phone company and a small network of service providers have access

38. 442 U.S. 735 (1979).
39. *See id.* at 736 n.1 (explaining that a pen register records the telephone numbers one dials but does not transmit conversation) (citations omitted).
40. *Id.* at 736.
41. *Id.* at 742.
42. *Id.*
43. *See id.* (reasoning that callers know they are conveying dialed numbers to the phone company and that the phone company makes permanent records of calls because of long distance billing).
44. *Id.* at 743.

to this information. The physical infrastructure of the telephone network does not allow observation of its workings—not without significant trespasses onto telephone company property or burglary of its buildings. Explicit and implicit contract terms (based on telephone companies' privacy-related representations) contribute legal backing to the privacy of telephone dialing information, as do any number of regulations.[45]

Smith was a bad decision for proponents of privacy and a strong Fourth Amendment. But more importantly here, *Smith* revealed the doctrinal weakness of the test Justice Harlan proposed in *Katz*. The Court could have come to any conclusion within the rubric of the test. It is no guide at all.

The Circularity of Harlan's Katz *Test*

The slipperiness of Justice Harlan's formulation is compounded by its essential circularity. Societal expectations are guided by judicial rulings, which are supposedly guided by societal expectations, which in turn are guided by judicial rulings, and so on. This is another sense in which the Fourth Amendment is left without a foundation by Harlan's *Katz* test.

Its circularity is especially problematic here at the onset of the Information Age. With Internet communications only beginning to take their place in society, expectations about privacy on this medium are just beginning to take form. Accordingly, a battle over Fourth Amendment "expectations" has broken out. If proponents of government surveillance can mold expectations to their advantage, they can have broad access to communications. Unsurprisingly, they have sought to do so.

Speaking at a conference in October 2007, for example, Principal Deputy Director of National Intelligence Dr. Donald Kerr said,

> Too often, privacy has been equated with anonymity; and it's an idea that is deeply rooted in American culture. . . . But in our interconnected and wireless world, anonymity—or the appearance of anonymity—is quickly becoming a thing of the past . . . . Protecting anonymity isn't a fight that can be won. Anyone that's typed in their name on Google understands that. Instead, privacy, I would offer, is a system of laws, rules, and customs with an infrastructure of Inspectors General, oversight committees, and

45. *See, e.g.*, 47 U.S.C. § 222 (1996). Section 222, entitled "Privacy of Customer Information," was added to the Communications Act by the Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996) (codified in scattered sections of 47 U.S.C. (2000)).

> privacy boards on which our intelligence community commitment is based and measured.[46]

This is privacy not as control, consistent with the *Katz* majority. It is privacy as due process—after control has been taken away. Were this view of privacy to take hold, Internet users could not expect limits on government access to the personal information they transmit. Rather, their Fourth Amendment "rights" would be opportunities to appeal to oversight boards regarding appropriate use of the information governments maintain about them.

This is not the Fourth Amendment we know, of course; nor is it the one the Supreme Court majority applied in *Katz*. The weakness of current Fourth Amendment doctrine allows national security officials to convince themselves that wholesale access to Americans' communications is consistent with the Constitution.

4 + 1 = 4?

Communications privacy is under heavy siege in the post-September 11, 2001 environment. Perhaps, it has been argued, the Fourth Amendment can be strengthened by importing First Amendment considerations. Alas, using "chilling effects" analysis to bolster the Fourth Amendment is not likely to work.

Some truly bright lights have advocated for this approach. Harvard Professor Laurence Tribe, for example, discussed curing the circularity of Harlan's approach in an August 2007 speech to the Progress and Freedom Foundation's Aspen Summit:

> It turns out that to break through the circle and to give content to the Fourth Amendment of the Constitution, you have to pay attention to the First Amendment of the Constitution. The Court didn't discuss the matter in any great detail, but the basic point it made was that because electronic communications are central to a system of free expression, there would be an unacceptable chilling effect on the freedom of speech if people believed the government was overhearing all their conversations.[47]

Indeed, the majority opinion in *Katz* briefly glanced toward First Amendment territory: "To read the Constitution more narrowly is to

---

46. Dr. Donald Kerr, Principal Deputy Dir. of Nat'l Intelligence, Remarks and Q&A at the 2007 Geospatial Intelligence (GEOINT) Symposium (Oct. 23, 2007), http://www.dni.gov/speeches/20071023_speech.pdf.

47. Laurence H. Tribe, Carl M. Loeb Univ. Professor, Harvard Law Sch., Freedom of Speech and Press in the 21st Century: New Technology Meets Old Constitutionalism, Plenary Address Before the Progress and Freedom Foundation Aspen Summit (Aug. 20, 2007), http://www.pff.org/issues-pubs/pops/pop14.19tribe transcript.pdf.

ignore the vital role that the public telephone has come to play in private communication," it said.[48]

But chilling effects tests would not be much use when tough calls are made on surveillance—especially secret surveillance. Adding First Amendment considerations to the Fourth Amendment test conceived by Justice Harlan does not restore or recharge the Fourth Amendment, as an example helps to illustrate.

Anderson v. Sills[49] was a case that premised its holding on the assumption that government surveillance has chilling effects on speech, association, and the press. In the wake of urban rioting in 1967, the New Jersey Attorney General issued a memorandum encouraging broad surveillance and intelligence collection programs aimed at potential troublemakers. Civil rights activists and the Jersey City NAACP sued, asserting that the policy violated the First Amendment. The New Jersey Superior Court agreed, holding the system unconstitutional.

In 1969 the New Jersey Supreme Court reversed,[50] but not before the *Harvard Law Review* produced a note that did a good job of unpacking the factors that might govern the relationship between surveillance and chilling effects:

> Four components of the "chilling effect" can be identified: the public knowledge of the system's existence, the nature of the information collected, the methods by which it is gathered, and the way in which it may eventually be used.[51]

This suggests a four-factor test that might govern First Amendment claims against surveillance activities. As we have seen, though, *x*-factor tests are weak law. As often as not, they drape policymaking in black robes. And other policy priorities can easily trump the "chilling effects" argument for Fourth Amendment privacy while fear of terrorism, legitimate or exaggerated, dominates the discourse.

Consider how widespread, nominally secret, surveillance of Americans' communications would fare under the *Anderson-Harvard Law Review* four-part test if it were applied by Judge Richard Posner of the United States Court of Appeals for the Seventh Circuit. In late 2005, Posner editorialized in the *Washington Post* defending large-scale communications surveillance after it had begun to come to

48. Katz v. United States, 389 U.S. 347, 352 (1967).
49. 256 A.2d 298 (N.J. Super. Ct. Ch. Div. 1969), *rev'd*, 265 A.2d 678 (N.J. 1970).
50. *See Anderson*, 265 A.2d at 687 ("If a properly drawn measure is within the power of government, it is no objection that the exercise of speech or association is thereby 'chilled.'").
51. *Recent Cases*, 83 HARV. L. REV. 935, 938 (1970).

light.[52] His thinking illustrates how secret mass surveillance might fare under "chilling effects" analysis.[53]

Public knowledge of the system's existence

Public knowledge leads to chilling effects, and secrecy avoids them, so the secrecy of surveillance under a chilling effects test would be a feature—not a concern. Truly secret surveillance cannot chill the speech of anyone but the paranoid.

Nature of the information collected

As to the nature of the information collected, Posner would assess it as follows: "[T]he data are first sifted by computers, which search for names, addresses, phone numbers, etc., that may have intelligence value."[54] As far as can be known when surveillance practices are secret, only common identifiers are examined, and only legitimate subjects of investigation are really inspected. The nature of the information was not a concern to Posner.

Methods by which it is gathered

Surveillance that is electronic also avoids chilling effects. As to privacy, Posner observed, "machine collection and processing of data cannot, as such, invade privacy. . . . [The] initial sifting, far from invading privacy (a computer is not a sentient being), keeps most private data from being read by any intelligence officer."[55] The same would apply to the question of chilling speech. If a machine cannot invade privacy, such a machine cannot chill speech either. Score another one for mass electronic surveillance.

Eventual use

Would such data be subject to future misuse, such as blackmail or intimidation of political enemies? "That danger is more remote than at any previous period of U.S. history,"[56] said Posner, citing increased political partisanship, advances in communications technology, and

52. Richard A. Posner, Editorial, *Our Domestic Intelligence Crisis*, WASH. POST, Dec. 21, 2005, at A31.

53. *See, e.g.*, Stephen M. Johnson, *Bringing Deference Back (But for How Long?): Justice Alito,* Chevron, Auer*, and* Chenery *in the Supreme Court's 2006 Term*, 57 CATH. U. L. REV. 1, 43 (2007) (observing that the Supreme Court's multi-factor tests "can be manipulated to reach the outcome that the Court desires").

54. *Id.*

55. *Id.*

56. *Id.*

the competitive media landscape to find that abuses would not occur.[57]

These arguments rely on countless assumptions about the design of surveillance systems and the beneficence of those operating them, of course. Such forgiving analysis is required by indulgence of government secrecy. All the same, it shows how surveillance can be argued—credibly enough for a national newspaper—not to chill free speech.

Propping up the Fourth Amendment with the First also does not protect against other privacy depredations that advances in government surveillance technology might bring. For example, scanning technology now allows examination of the contents of people's pockets and bags as they pass through doorways and entrances. Used first at airports, the technology might make its way to government checkpoints at bus stations, subways, shopping malls, and museums. After a time, courts could be persuaded that society does not support an expectation of privacy in possessions that are carried in public, even though they are concealed.

There is no communicative content to carrying things inside a bag, of course, so there would be no argument supporting the Fourth Amendment privacy of such things based on the "chilling effects" of examining carried items. First Amendment considerations do not protect privacy against erosion along this dimension.

Along with the malleability of "chilling effects" analysis, the fortitude given to the Fourth Amendment by First Amendment considerations is too limited in scope. The Fourth Amendment must stand on its own. And, happily, it can.

Enter Kyllo

The Supreme Court has rendered at least one Fourth Amendment decision post-*Katz* that is consistent with that case's actual holding. *Kyllo* might be too easily dismissed as a "high-tech" case, but it explores the same interplay of privacy and technology that was at

57. *See id.* One is reminded of Justice Scalia's observation in *Hudson v. Michigan*, 547 U.S. 586, 598 (2006), on the "increasing professionalism of police forces, including a new emphasis on internal police discipline." Blogger Radley Balko has endlessly derided this assumption in posts covering wrong-door raids, use of Tasers in response to impudence, cover-ups of official or unofficial police misconduct, and—a Balko favorite—puppycide: raids in which law enforcement officers kill the family dog. *See* Postings of Radley Balko to http://www.theagitator.com/category/police-professionalism/. *See generally* Radley Balko, *Overkill: The Rise of Paramilitary Police Raids in America* (The Cato Inst., Washington, D.C.), July 17, 2006, *available at* http://www.cato.org/pubs/wtpapers/balko_whitepaper_2006.pdf.

issue in *Katz* and that dominates government surveillance debates today.

In *Kyllo*, agents of the U.S. Department of the Interior, suspicious that Danny Lee Kyllo was growing marijuana in his home using high-intensity lamps, aimed an Agema Thermovision 210 thermal imager at his triplex on Rhododendron Drive in Florence, Oregon.[58] The imager detected significantly more heat over the roof of the garage and on a side wall of Kyllo's home than elsewhere on the premises. Using this and other information, the agents got a warrant, searched the home, and found the drugs they suspected.[59]

The "War on Drugs" has pushed law enforcement to test the limits of its search and surveillance powers in many respects, and the Supreme Court has not always defended Americans' privacy rights as it should. In this case, however, despite the presence of drugs, the Supreme Court found a Fourth Amendment violation and remanded Kyllo's conviction.[60]

"Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion," Justice Scalia wrote for the Court, "the surveillance is a 'search' and is presumptively unreasonable without a warrant."[61]

Like Katz had done by entering a telephone booth, Kyllo had used the walls of his house to shield from others the interior temperature of its rooms. Thermal imagers are not in general public use, so people desiring to keep the hours of their sauna private from neighbors need not line their walls with asbestos. As a matter of fact—not expectation or "objective" opinion—Kyllo had privacy in the fact that there were high temperatures in some rooms of his home. When the government used out-of-the ordinary efforts to overcome that, it was unreasonable and it violated his Fourth Amendment rights.[62]

This is the majority holding in *Katz*—that a person who has concealed information from the general public has concealed it from the government. Other than in certain narrow cases such as exigency, the government cannot overcome his or her privacy except by getting a warrant. The privacy finding is a single, fact-based

58. 533 U.S. 27, 29 (2001).
59. *Id.* at 30.
60. *Id.* at 40–41.
61. *Id.* at 40.
62. *Id.*

inquiry, not the subjective-"objective" two-part test that Harlan thrust upon *Katz*.

Though it is a single inquiry, it may not always be an easy one. Technologies for collecting information will continue to propagate into society, altering the steps that must be taken to control information. There are already reasonably priced video cameras that have infrared functionality, for example. At some point (perhaps already), they may be common enough to reverse the holding of the *Kyllo* case without disturbing its rationale.

As technologies like this press more tightly against the laws of physics, privacy practices and expectations may change, but courts need not guess at these questions, which have societal sweep. In each case, the question whether a person has maintained privacy in particular information is a factual inquiry.

Privacy is a Factual Question

The *Katz* holding calls for the following factual inquiry in Fourth Amendment cases: Did the individual claiming Fourth Amendment protection actually have privacy in the information he or she claims the government should not have accessed without a warrant? Was the information available to others or not? If the information was not generally available—if it was private—the question is whether the government was reasonable in accessing it without a warrant, which will rarely be the case.

People going about their daily lives constantly create information. Pieces of personal information are produced by each and every exercise of cognition and volition. Much of this information is never consciously observed or recorded.[63] Some of this information is abandoned to the world as it is created.[64] When a person walking on the street wears a bright yellow hat, for example, the fact of his or her walking and wearing a yellow hat is available to anyone who might bother to collect it and use it. It is not private.

But when a person walking on the street carries an aspirin tablet in a coat pocket, that fact is not available to anyone. The physical

63. Perhaps there are philosophical questions about whether information exists in the absence of anyone taking notice of it.

64. *See generally* Jim Harper, Dir. of Information Policy Studies, Cato Inst., Remarks at Cato Institute Conference on Copyright Controversies: Freedom, Property, Content Creation, and the DMCA (Apr. 26, 2006), *in* 28 CATO POLICY REPORT 15–16 (July/Aug. 2006), *available at* http://www.cato.org/pubs/policy_report/v28n4/cpr-28n4-4.pdf (contrasting the default rule in physical property of exclusivity with the default rule in personal information that "what is observable by others is public").

barrier of the fabric prevents others from gaining access to that information. The person can share the information by telling others or by letting them see the pill drop in the pocket, but, otherwise, the contents of the pocket are not known. That information is private—as a matter of objective fact.

Often, privacy is protected by a combination of both physical barriers and common law rights. The pill in the pocket cannot be discovered while the owner wears the coat without someone committing at least a minor battery. Inside the home, privacy is protected by real property law, which excludes the unwelcome from places where they might learn private information.

The question gets more complicated when objects or information are entrusted to others. Leaving a coat on a coat rack in a coffee shop may permit someone to examine its pockets' contents and learn the information. Privacy may be lost without the individual's permission, yet without any violation of his or her rights. Leaving the same coat inside a home would allow people rightfully there to discover the pill, but not trespassers.

People often protect information by contract, of course. Many contracts have explicit or implied terms having to do with personal information. The information-terms of contracts for financial services, telecommunications, and other goods and services have not been thoroughly explored by privacy advocates or the legal academy, but as a general matter information produced by such transactions is not widely or publicly available, even while it is shared within a small universe of service providers consistent with the interests of the parties.

Statutes and regulations sometimes protect privacy, though the totality of regulation probably does more to undermine it.[65] An issue of disagreement among the justices in *Olmstead*, which may seem peripheral to readers decades later, is central to the Court's error in that case. Statutory law in Washington State forbade intercepting, reading, or interrupting any message sent by telegraph or telephone.[66] Among other ends, this law protected the privacy of Olmstead and his cohorts. The general public could not legally access the content of their conversations so, contrary to the holding

65. *See generally* JIM HARPER, CATO INSTITUTE POLICY ANALYSIS NO. 520: UNDERSTANDING PRIVACY—AND THE REAL THREATS TO IT (2004), *available at* http://www.cato.org/pubs/pas/pa520.pdf (classifying government threats to privacy into three groups: (1) government surveillance, (2) collecting and sharing personal information about citizens for administrative purposes, and (3) laws that degrade citizens' power to protect privacy as they see fit).

66. *See* Olmstead v. United States, 277 U.S. 438, 468–69 (1928).

of the case, the government could not do so either, constitutionally, unless it got a warrant.

A recent case in the Unites States Court of Appeals for the Eleventh Circuit illustrates how treating privacy as a factual question can simplify things while leading to sound judgments. In *United States v. King*,[67] the defendant had attached his computer to a military network from his dorm room, unknowing that his computer's security settings allowed sharing his files with the entire network.[68] A military computer specialist on the network, happening across his files, discovered child pornography and reported it.[69]

Carefully applying the doctrine that has grown up around the *Katz* decision, the court of appeals walked through the two-step inquiry into whether defendant King should have privacy in his computer files recognized under the Fourth Amendment.[70] Granting that he subjectively (if mistakenly) expected privacy, the court found that it was not something that society could accept as objectively reasonable:

> It is undisputed that King's files were "shared" over the entire base network, and that everyone on the network had access to all of his files and could observe them in exactly the same manner as the computer specialist did. As the district court observed, rather than analyzing the military official's actions as a search of King's personal computer in his private dorm room, it is more accurate to say that the authorities conducted a search of the military network, and King's computer files were a part of that network. King's files were exposed to thousands of individuals with network access, and the military authorities encountered the files without employing any special means or intruding into any area which King could reasonably expect would remain private.[71]

These facts allow feelings, opinions, and "reasonable expectations" to be put aside: King had not protected privacy in his computer files; thus, their content was not protected by the Fourth Amendment.

The question whether a person has privacy is a matter of objective fact, determined by whether others could physically and legally gain access to the information. Many privacy values are shared, which leads people to believe that societal "expectations" should govern Fourth Amendment cases, but the existence or non-existence of privacy in particular information at a given time and place is a factual question.

---

67. 509 F.3d 1338 (11th Cir. 2007).
68. *Id.* at 1339.
69. *Id.* at 1339–40.
70. *Id.* at 1341–42.
71. *Id.* at 1342.

Armed with this knowledge, courts can be much more clear that surveillance of communications is not to be conducted without warrants. Americans entrust information about themselves to Internet service providers and telephone companies knowing that the physical plant across which their messages pass is not open to public access. Implied and explicit contract terms govern exactly what may be done with the information, and statutory law does as well.

The Internet is not a "cloud" that rains information at random across the plains. It is not an information stew from which anyone can ladle out the morsels that interest them. Thanks to the Fourth Amendment and the holding in *Katz*, government officials do not hold a ladle unless a judge gives them a limited-purpose one in the form of a warrant.

Ending the "Third Party Doctrine"

Another thread of Supreme Court doctrine joins Justice Harlan's gloss on *Katz* to undermine privacy, the Fourth Amendment, and the nation's confidence in its freedom. This is the "third-party doctrine."

In the 1970s, a pair of cases arising from the Bank Secrecy Act[72] ("BSA") did an extraordinary sidestep around the Fourth Amendment protections that the Court should have used to restrain the government's investigatory activities under that law.

The first case is *California Bankers Association v. Shultz*.[73] In this case, the Court denied challenges brought by several parties to the BSA requirement that banks maintain records and file reports with the Treasury Department that "have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings."[74]

The information-collection part of the law does not require disclosure to the government, so the Court denied in *California Bankers* that it implicates the Fourth Amendment. "[T]he mere maintenance of the records by the banks under the compulsion of the regulations invade[s] no Fourth Amendment right . . . ."[75] As to the reporting requirements, the Court denied standing to bank depositors who could not show that information about their financial transactions had been reported.[76]

72. Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114 (codified as amended at 12 U.S.C. §§ 1951–1959. (2000)).
73. 416 U.S. 21 (1974).
74. 12 U.S.C. § 1829b(a)(2) (2000).
75. *Cal. Bankers Ass'n*, 416 U.S. at 54.
76. *Id.* at 67–68.

There were a number of strong dissents. Justice Marshall presciently criticized how the Court avoided finding that mandated record-keeping affects a constitutional seizure just because the government would acquire the records later. "By accepting the Government's bifurcated approach to the recordkeeping requirement and the acquisition of the records, the majority engages in a hollow charade whereby Fourth Amendment claims are to be labeled premature until such time as they can be deemed too late."[77]

Sure enough, in *United States v. Miller*,[78] the Court held that a defendant had no Fourth Amendment interest in records maintained about him pursuant to the BSA.[79] Like the *Smith* court, the *Miller* Court slipped up on Justice Harlan's gloss on *Katz*:

> Even if we direct our attention to the original checks and deposit slips, rather than to the microfilm copies actually viewed and obtained by means of subpoena, we perceive no legitimate "expectation of privacy" in their contents.[80]

The two-step was complete. Under these cases, the government can compel a service provider to maintain records about a customer and then collect those records without implicating his or her Fourth Amendment rights.

These holdings were never right, but they grow more wrong with each step forward in modern, connected living. Incredibly deep reservoirs of information are constantly collected by third-party service providers today.

Cellular telephone networks pinpoint customers' locations throughout the day through the movement of their phones. Internet service providers maintain copies of huge swaths of the information that crosses their networks, tied to customer identifiers. Search engines maintain logs of searches that can be correlated to specific computers and usually the individuals that use them. Payment systems record each instance of commerce, and the time and place it occurred.

The totality of these records are very, very revealing of people's lives. They are a window onto each individual's spiritual nature, feelings, and intellect. They reflect each American's beliefs,

77. *Id.* at 97 (Marshall, J., dissenting).
78. 425 U.S. 435 (1976).
79. *Id.* at 442–43.
80. *Id.* at 442.

thoughts, emotions, and sensations. They ought to be protected, as they are the modern iteration of our "papers and effects."[81]

CONCLUSION

There can be little doubt that surveillance has chilling effects, but this does not create strong legal arguments that will reliably prop up Fourth Amendment search and seizure law. Importing the First Amendment into the Fourth using "chilling effects" arguments can be trumped by other policy considerations.

Rather, Fourth Amendment doctrine should be reconstituted and made to stand on its own. The *Katz* case has all that courts need to do just that. The majority holding in the case found that the maintenance of privacy in information was sufficient to garner Fourth Amendment protection.

Privacy is not a question of law, but of fact. If information is not available to others, it is private, and the Fourth Amendment protects it. Only reasonable efforts to get personal information will pass constitutional muster, and these typically require a warrant.

Restoration of this rule would right the one-way ratchet Justice Harlan mistakenly injected into Fourth Amendment doctrine through his concurrence in *Katz*. Under his two-part test, the privacy of information is second-guessed by courts using an unworkable "reasonableness" test.

The Fourth Amendment takes the individual's circumstances as a given (including his or her privacy) and asks whether the government has been reasonable. It does not ask whether Americans' privacy is reasonable. Current Fourth Amendment doctrine has it backward. It should be reformed.

81. *See* U.S. CONST. amend. IV (declaring that people have the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures").