WHY THE NSA DATA SEIZURES ARE UNCONSTITUTIONAL

RANDY BARNETT*

Due to the unauthorized leaks of classified information, we have come to learn that the National Security Agency (NSA), an executive branch arm of the U.S. military, has established several data collection programs. In this article, I am not going to get into the details of these programs. Instead, I will limit my focus to what I consider to be the serious constitutional problem with any such program, regardless of the details: the fact that the NSA is demanding that private companies, with which virtually all Americans contract to provide their voice communications, turn over the records of every phone call that is made on their systems.[1] This metadata is then stored on NSA super computers for later analysis.[2]

In this article, I am not going to address the legality of this program under existing statutes. Jim Harper of the Cato Institute and I have argued in an amicus brief that the NSA data collection program is illegal because it is not authorized by Section 215 of the Foreign Intelligence and Surveillance Act as it was modified by the USA PATRIOT Act.[3]

---

* Carmack Waterhouse Professor of Legal Theory, Georgetown University Law Center. Director, Georgetown Center for the Constitution. This essay was adapted from remarks given at the 2014 Federalist Society Annual Student Symposium at the University of Florida in Gainesville, Florida.

1. *See* Michael J. Glennon, *National Security and Double Government*, 5 HARV. NAT'L SEC. J. 1, 7 (2014); Andrew William Bagley, *Don't Be Evil: The Fourth Amendment in the Age of Google, National Security, and Digital Papers and Effects*, 21 ALB. L.J. SCI. & TECH. 153, 156–57 (2011).

2. *See, e.g.*, Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN (June 5, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [http://perma.cc/5EAX-73CA].

3. Brief of Amicus Curiae Cato Institute in Support of Petitioner, *In re* Privacy Info. Ctr., 134 S. Ct. 638 (2013) (No. 13-58) *available at* http://object.cato.org/sites/cato.org/files/pubs/pdf/tsac_cato_institute_13-58.pdf [http://perma.cc/HU3V-8LYH].

Section 215 of the PATRIOT Act allows the Foreign Intelligence Surveillance Court (FISC) to issue orders requiring the production of tangible things upon satisfactory application by the FBI. The statutory language specifies that an application for a Section 215 order must include "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation . . . ."[4] Because we maintain that Section 215 orders must be "relevant" to an already existing investigation, in our brief we contended that orders for the seizure of bulk metadata on every American for future analysis to uncover evidence of wrong doing are not authorized by the statute and are therefore illegal.[5]

So far, however, the two federal district court judges who have considered challenges to the program in the Southern District of New York and in the District of Columbia have both held that, because Congress has not waived its sovereign immunity to allow the legality of Section 215 orders to be challenged in federal court, federal courts lack jurisdiction to hear a statutory challenge.[6] For this reason, this matter may need to be addressed by Congress. But these same two judges also held that citizens have standing to bring constitutional challenges to the collection of the telephone companies' records of their phone calls.[7] So my focus here will be limited to the constitutional issue raised by these blanket seizures of the private data on all Americans.

Although the only surveillance program that has been challenged thus far concerns phone records,[8] the principle offered to support this data seizure applies as well to all other business records of our dealings, including our credit card transactions. Indeed, in upholding the constitutionality of the program, Judge William Pauley of the Southern District of New York cited cases that held that "an individual has no constitutionally protected expectation of privacy" in bank records, records given to an accountant, subscriber information provided to an internet service provider, and information from a home comput-

4. 50 U.S.C. § 1861(b)(2)(A) (2012).

5. Cato Institute, *supra* note 3, at 3–5.

6. Klayman v. Obama, 957 F. Supp. 2d 1, 9 (D.D.C. 2013); ACLU v. Clapper, 959 F. Supp. 2d 724, 742 (S.D.N.Y. 2013).

7. *Klayman*, 957 F. Supp. 2d at 9; *Clapper*, 959 F. Supp. 2d at 742–49.

8. *Klayman*, 957 F. Supp. 2d at 7; *Clapper*, 959 F. Supp. 2d at 730.

er that is transmitted over the Internet or by email.[9] Imagine the chilling effect on liberty if everyone knew that the government is in possession of all this data about their private transactions on its super computers. The relationship between the citizens of the United States and their supposed agents or servants in government would be fundamentally reversed, turning We the People into mere subjects of our rulers.

So there is a lot more at stake here than just this particular bulk data seizure program. With the challenge to the Affordable Care Act, we not only wanted to stop Obamacare from being implemented—which sadly we failed to do—we also wanted to defeat the limitless constitutional arguments that were being offered in its defense. In this effort, I am pleased to say we succeeded.[10] Now, we need to think very hard about whether these blanket data seizure programs comport with the Fourth Amendment before, not after, the government decides it needs to seize data about every facet of our personal lives.

I. BLANKET DATA SEIZURES ARE MODERN DAY GENERAL WARRANTS

The Fourth Amendment has two parts. First, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[11] And second, "no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[12]

We know that the Fourth Amendment was adopted to prevent, among other things, what were called "general" or nonspecific warrants, which were blanket authorizations for British authorities to search for contraband wherever they might choose. In response to this abuse, the Fourth Amendment re-

9. *Clapper*, 959 F. Supp. 2d at 749–51, n.16.

10. *See* Randy E. Barnett, *No Small Feat: Who Won the Health Care Case (And Why Did So Many Law Professors Miss the Boat)?*, 65 FLA. L. REV. 1331, 1333 (2013).

11. U.S. CONST. amend. IV.

12. *Id.*

quires the things to be searched or seized under a warrant to be described "particularly."[13]

With this in mind, the problem with the data collection orders issued to Verizon and other telecommunications companies becomes obvious. These orders require the company to produce "on an ongoing daily basis . . . all call detail records."[14] Because they are not "particular," such orders are the modern incarnation of the general warrants issued by the Crown. As with general warrants, blanket seizure programs subject the private information of innocent people to the risk of searches and exposure, without their knowledge and with no realistic prospect of a remedy.

It is also worth remembering that both the English Whigs and the American Founding generation thought that the seizure of papers for *later* search was an abuse distinct from, but equivalent to, the use of general search warrants—which is why "papers" was included in the Fourth Amendment in addition to "effects" or personal property.[15] As University of San Diego School of Law Professor Donald Dripps has shown in a recent article, "at the heart of Whig opposition to seizing papers was the belief that *any* search of papers, even for a specific criminal item, was a *general search*. It followed that any warrant to sift through documents is *a general warrant*, even if it is specific to the location of the trove and the item to be seized."[16] The seizure of one's papers for later perusal was thought to be closely akin to searching through a person's mind to assess his thoughts. Seize first, then search for evidence of criminality, was considered to be the epitome of an abuse of power.[17] Putting such information permanently in the hands of government for future use is an invitation to restrict the liberties of the people whenever such restrictions become politically popular.

---

13. *See* Morgan Cloud, *Searching Through History; Searching For History*, 63 U. CHI. L. REV. 1707, 1727–28, 1731 (1996).

14. Klayman v. Obama, 957 F. Supp. 2d 1, 10 (D.D.C. 2013) (citation omitted).

15. *See generally* Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure,* 103 J. CRIM. L. & CRIMINOLOGY 49 (2013) (explaining how the seizure of papers to be later searched for evidence of criminality was considered to be a distinct but equally disturbing abuse from that of general warrants to search houses).

16. *Id.* at 104.

17. *See id.* at 67.

For example, gun rights advocates have long opposed firearms registration because the brute fact that the government does not know where the guns are makes it much more difficult to confiscate them in the future.[18] Not only does this illustrate the practical danger to constitutional liberties posed by the government simply possessing vast information about our activities and associations for later search. The trove of phone and email metadata to which the NSA now has access would make gun registration unnecessary as the government would already possess enough information to identify most gun owners.[19]

A. Problems with the Constitutional Justifications of These Programs

So how have these programs been justified as constitutional? The answer lies in two key Supreme Court cases. The first is the 1967 case of *Katz v. United States*,[20] which concerned the power of law enforcement to wiretap a public phone booth.[21] *Katz* is taken to stand for the proposition that the Fourth Amendment protects only communications about which people have a "reasonable expectation[] of privacy."[22] Because people reasonably expect their conversations in a phone booth to be private, their conversations cannot be wire-tapped by law enforcement without first obtaining a search warrant.[23] Keep that phrase "reasonable expectation of privacy" in mind, because it does a lot of work in modern constitutional doctrine.

The second key case is *Smith v. Maryland*,[24] decided in 1979. *Smith* applied what is called the "third-party doctrine" to phone call information in the possession of phone companies.[25] In *Smith*, the Court reasoned that individual phone users have no reasonable expectation of privacy in the records of their

---

18. Nicholas J. Johnson, *Imagining Gun Control in America: Understanding the Remainder Problem*, 43 WAKE FOREST L. REV. 837, 868–69 (2008).

19. *See* Chris W. Cox, *The Battle Against Mass Government Surveillance,* NRA (Feb. 6 2014), http://www.nrapublications.org/index.php/16924/political-report-48/ [http://perma.cc/P2Q6-V9DQ].

20. 389 U.S. 347 (1967).

21. *Id.* at 348–49.

22. *Id.* at 362 (Harlan, J., concurring).

23. *Id.* at 359, 367.

24. 442 U.S. 735 (1979).

25. *See id*. at 744–45.

phone calls—the numbers called and the duration of the calls—since phone users must know that a third party, the phone company itself, has access to this information. The Court therefore held that law enforcement agencies do not need a warrant to install what is called a "pen register" on a telephone account that records and reports the numbers called and the duration of the calls, but not the content of the conversations.[26]

When the Foreign Intelligence and Surveillance Court, responding to public concerns, released its previously secret opinion upholding the constitutionality of the NSA's data seizure program, we learned that it thought that "the production of telephone service provider metadata is squarely controlled by the U.S. Supreme Court decision in *Smith v. Maryland*."[27] The court reasoned that the NSA data collection orders are constitutional because all they collect is the very information in which *Smith* tells us that telephone consumers have no reasonable expectation of privacy under *Katz*.[28] On the surface, this logic seems rather persuasive, and indeed it has persuaded many legal experts and commentators, along with Judge Pauley of the Southern District of New York.[29]

But there is a big difference between what happened in *Smith* and what the NSA orders are doing. In *Smith*, a robbery victim had described to the police both her attacker and a 1975 Monte Carlo she saw near the scene of the robbery.[30] Afterward, she began receiving threatening and obscene phone calls from a man who said he was the robber.[31] During one phone call, the man asked her to step out onto her front porch, where she saw the 1975 Monte Carlo moving slowly past her home.[32] Later, the police spotted a man who met the victim's description of

---

26. *Id*. at 741–42.

27. *In re* Application of the F.B.I. for an Order Requiring Prod. of Tangible Things from [REDACTED], No. BR 13-109, 2013 WL 5741573, at *2 (FISC Aug. 29, 2013).

28. *Id*. at *3.

29. ACLU v. Clapper, 959 F. Supp. 2d 724, 751 (S.D.N.Y. 2013) ("[B]usiness records created by Verizon are not 'Plaintiffs' call records.' . . . When a person voluntarily conveys information to a third party, he forfeits his right to privacy in the information.").

30. *Smith*, 442 U.S. at 737.

31. *Id.*

32. *Id.*

her attacker driving a 1975 Monte Carlo in her neighborhood.[33] By tracing the license plate number, police learned that the car was registered in the name of petitioner, Michael Lee Smith.[34] They then asked the phone company to install a pen register at its central offices to record the numbers dialed from the telephone at his home.[35] Although the police did not obtain a warrant, they certainly had a reasonable suspicion that Mr. Smith had engaged in illegal activity.[36]

If the constitutionality of the NSA's bulk data seizure programs is to be justified as akin to a pen register under *Smith*, however, then these programs amount to installing a pen register on every American without any suspicion that a person, whose phone activities are now stored on the NSA's supercomputers, has done anything wrong.[37] In essence, every American is to be treated the way Michael Lee Smith was treated in *Smith v. Maryland*.[38] But unlike the pen register on his phone line that lasted just a few days, each of us would have pen registers on our phone every day for the rest of our lives.

In the old days, the government had to go to the third party to request the pen register be installed,[39] which preserved a record of what it was doing. Moreover, had it tried to collect such information on everyone, the very massiveness of such a data trove would have itself prevented the government from storing it or doing much of anything else with it. Today, however, enormous quantities of data can be kept digitally in huge NSA facilities.[40]

---

33. *Id.*

34. *Id.*

35. *Id.*

36. *Id.*

37. *See* Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757, 869 (2014).

38. *Id.*

39. *See* United States v. N.Y. Tel. Co., 434 U.S. 159, 162 (1977) (noting that telephone company refused to lease certain telephone lines to the FBI which were needed to install a pen register discretely).

40. Howard Berkes, *Amid Data Controversy, NSA Builds Its Biggest Data Farm*, NPR (June 10, 2013, 2:58 AM), http://www.npr.org/2013/06/10/190160772/amid-data-controversy-nsa-builds-its-biggest-data-farm [http://perma.cc/7XKJ-MLF5]; *NSA Utah Data Center*, UTAH FACILITIES (Sept. 14, 2011), http://www.facilitiesmagazine.com/utah/buildings/nsa-utah-data-center [http://perma.cc/797Q-522F].

In its briefs, the government intimates that the NSA is subjecting the data to computer analysis to reveal suspicious patterns.[41] But others have defended the retention of this data simply to facilitate future searches of records pursuant to later investigations.[42] Once in possession of the data, however, the federal government can use it the same way British authorities used papers seized with general warrants for later perusal to see if they revealed anything criminal. The NSA data seizures make possible fishing expeditions into the phone calling patterns of nearly all Americans, except for terrorists, who will now avoid using their phones.[43]

If this is the result, then there must be a flaw somewhere in the constitutional doctrine that produced it. And indeed the fault lies in the misuse of the "third-party doctrine" as well as in *Katz*'s problematic concept of the reasonable expectation of privacy.

B. Misapplying Katz *and* Smith

The key to understanding the flaw in the government's theory is to remember that the Fourth Amendment was, above all else, the solution to the problem of general or nonspecific warrants.[44] In *Smith v. Maryland*,[45] a pen register was placed by the phone company on a particular person about whom there was a reasonable suspicion—though perhaps not probable cause for seeking a search warrant.[46] Indeed, previous applications of the third party doctrine to business records, such

---

41. Defendants' Memorandum in Opposition to Plaintiffs' Motion for Preliminary Injunction at 1, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (1:13-cv-03994-WHP), 2013 WL 5744828; Brief for the United States in Opposition at 7–8, *In re* Elec. Privacy Information Ctr., 134 S. Ct. 638 (2013) (No. 13-58), 2013 WL 5702390.

42. *See, e.g.*, Roger Pilon & Richard A. Epstein, *NSA surveillance in perspective*, CHICAGO TRIBUNE, June 12, 2013, http://articles.chicagotribune.com/2013-06-12/opinion/ct-perspec-0612-nsa-20130612_1_nsa-national-security-agency-privacy [http://perma.cc/WM7B-UV66]; Dianne Feinstein, *NSA Call-Records Program Is Prudence, Not Prying*, SFGATE (Nov. 2, 2013, 8:58 PM), http://www.sfgate.com/opinion/article/NSA-call-records-program-is-prudence-not-prying-4947762.php [http://perma.cc/EK22-5Y3H].

43. *See* Barbara Starr, *Terrorists try changes after Snowden leaks, official says*, CNN (June 25, 2013, 6:27 PM), http://security.blogs.cnn.com/2013/06/25/terrorists-try-changes-after-snowden-leaks-official-says/ [http://perma.cc/7TT2-5FY3].

44. Cloud, *supra* note 13, at 1727–31.

45. 442 U.S. 735, 741–42 (1979).

46. *Id.* at 741–42.

as bank records or emails, have concerned investigations of a *particular person or company*.[47]

So the first problem is that *Smith v. Maryland* is being stretched to cover a situation that is radically different than the law enforcement practice the Court was addressing there, and in subsequent cases. Because this ongoing blanket data seizure of every phone record in the country is unprecedented, the rationale of *Smith* cannot automatically be extended to this situation.

This was the position taken by Judge Richard Leon of the District Court of the District of Columbia in his opinion finding that the NSA program violated the Fourth Amendment. "The question before me," he wrote,

> is *not* the same question that the Supreme Court confronted in *Smith*. To say the least, "whether the installation and use of a pen register constitutes a `search' within the meaning of the Fourth Amendment,"—under the circumstances addressed and contemplated in that case—is a far cry from the issue in this case.[48]

For Judge Leon, the question to be decided today is:

> When do present-day circumstances—the evolutions in the government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies—become so thoroughly unlike those considered by the Supreme Court thirty-five years ago that a precedent like *Smith* simply does not apply? The answer, unfortunately for the Government, is now.[49]

While lower courts are certainly bound to follow Supreme Court precedent, they are not required to extend general statements made by the Court in one situation to an entirely different context. Lower courts are supposed to grapple with applying existing doctrine to new situations, and this includes identifying the limits of existing doctrine given the circumstances in which it arose.

The crucial constitutional difference between *Smith* and all the "third-party" business records cases is *particularity*: the difference between a general warrant that the Fourth Amendment

---

47. *See* Donohue, *supra* note 37, at 865–71.

48. Klayman v. Obama, 957 F. Supp. 2d 1, 31 (D.D.C. 2013) (citations omitted).

49. *Id.*

was enacted to prohibit, and a reasonable particularized search or seizure, which is all the Supreme Court has ever purported to authorize.[50]

C. Reconsidering Katz

But when this case does get back to the Supreme Court—as I hope it will if Congress does not alter the practice as it recently failed to do[51]—the Court should also reconsider the "reasonable expectation of privacy" concept of *Katz*. As Justice Alito observed two terms ago in his concurring opinion in the GPS tracker case of *United States v. Jones*,[52] the "*Katz* expectation-of-privacy test . . . involves a degree of circularity, and judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks."[53] In addition, "the *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations."[54]

We should all remember that the "reasonable expectations" language that now dominates the academic literature and case law actually appears, not in the majority opinion of the Court in *Katz*, but in a solo-concurrence by Justice Harlan.[55] In contrast with Justice Harlan's concurrence, Justice Stewart's majority opinion in *Katz* properly rested on the physical protection that the defendant had given to his oral communications when he stepped into a phone booth and closed the door.[56] "What a person knowingly exposes to the public," he wrote "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."[57] What Katz "sought to exclude when he entered the booth," Justice Stewart continued,

---

50. *See* Donohue, *supra* note 37, at 786, 865–71.
51. *See* USA FREEDOM Act, S. 2685, 113th Cong. (2014).
52. 132 S. Ct. 945 (2012) (citations omitted).
53. *Id.* at 962 (Alito, J., concurring).
54. *Id.*
55. *Katz v. United States*,389 U.S. 347, 361 (1967) (Harlan, J., concurring).
56. *Id.* at 352 (majority opinion).
57. *Id.* at 351.

> 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. No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.[58]

Rather than airy and untethered judicial speculations about "reasonable expectations," the courts should return to the traditional—and more readily administrable—property and contract rights focus of Fourth Amendment protection that was reflected in the majority opinion in *Katz*. Courts should examine how people employ devices that function like the walls of the home, or the phone booth in *Katz*, to conceal digital information and preserve their privacy. An inquiry into the physical and legal barriers people have placed around their information, for example, by using passwords to restrict access to their email, or entering into terms of service contracts with third parties that include privacy protections, can generally answer whether they have held it close, and establish the threshold of personal security that the Fourth Amendment requires a warrant to cross. No distinction should be made between sealing a letter before handing it to the postman, taking a phone call in a secluded phone booth, password-protecting one's email, or selecting a communications company with a privacy policy.

In short, the "reasonable expectation of privacy" test reverses the inquiry required by the Fourth Amendment. For good reason, the Fourth Amendment uses a possessive pronoun—"their"—to describe the "persons, houses, papers, and effects" it protects. People's ownership of themselves and their things is an essential counterweight to state power. And by availing themselves of the law of property and contract, people create their own zones of privacy. In short, *first comes property and contract, then comes privacy*. With this in mind, let us return to *Katz*.

In reality, the physical and legal barriers people place around their information define both their actual and "reasonable" expectations of privacy and should provide the doctrinal touch-

58. *Id.* at 352.

stone of the search warrant requirement. Two terms ago in *United States v. Jones,* the Supreme Court took an important step in this direction when it held that the "reasonable expectation of privacy" formulation from *Katz* does not supplant the protection of one's property from unreasonable searches, but instead adds *additional* protections to these.[59] "[T]he Katz reasonable-expectation-of-privacy test," wrote Justice Scalia, "has been *added to*, not *substituted for*, the common-law trespassory test."[60]

And with regard to information of our private activity that is entrusted to third parties, the Court should now recognize that, when consumers enter into terms of service contracts, whether with telecommunications companies, banks, or credit card companies, containing privacy assurances, they "reasonably expect" their information to be used solely in ways specified in those policies.[61] As Justice Marshall observed in his dissenting opinion in *Smith*, "[t]hose who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[62]

When people put their information behind passwords, they "reasonably expect" it to be private, every bit as much as Mr. Katz did when he shut the door to the public phone booth.[63] As Justice Sotomayor noted in her concurring opinion in *Jones*, the third-party doctrine "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[64] The NSA's program of "pen registers for everyone" has shown how the conventional reading of *Katz*'s "reasonable expectation of privacy" test is patently unsuited for the age of mass storage of data accessed in secret and analyzed by super computers.

Indeed, it is useful to remember that Justice Stewart, the author of *Katz*, actually dissented in *Smith v. Maryland*. "I think

---

59. *Jones*, 132 S. Ct. at 952.

60. *Id.*

61. *See* Donohue, *supra* note 37, at 765 ("Americans do not expect that their telephony metadata will be collected and analyzed.").

62. *Smith*, 442 U.S. at 749 (Marshall, J., dissenting).

63. Donohue, *supra* note 37, at 890.

64. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

that the numbers dialed from a private telephone—like the conversations that occur during a call," he wrote,

> are within the constitutional protection recognized in *Katz*. It seems clear to me that information obtained by pen register surveillance of a private telephone is information in which the telephone subscriber has a legitimate expectation of privacy. The information captured by such surveillance emanates from private conduct within a person's home or office—locations that without question are entitled to Fourth and Fourteenth Amendment protection. Further, that information is an integral part of the telephonic communication that, under *Katz*, is entitled to constitutional protection, whether or not it is captured by a trespass into such an area.[65]

Presciently for purposes of analyzing the significance of installing pen registers for everyone, he added,

> The numbers dialed from a private telephone—although certainly more prosaic than the conversation itself—are not without "content." Most private telephone subscribers may have their own numbers listed in a publicly distributed directory, but I doubt there are any who would be happy to have broadcast to the world a list of the local or long distance numbers they have called. This is not because such a list might in some sense be incriminating, but because it easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life.[66]

When one has arranged one's affairs using physics, or the laws of property and contract, to conceal information from preying eyes, government agents may not use surreptitious means or novel technologies like thermal imaging to defeat those arrangements without obtaining a warrant that conforms to the requirement of the Fourth Amendment.[67] For this reason, the Court was correct in the 2001 case of *Kyllo v. United States*[68] to hold that police officers conducted a search when they used

---

65. *Smith*, 422 U.S. at 747–48 (Stewart, J., dissenting).

66. *Id.* at 748.

67. Hunter Carpenter, *Constitutional Law—Fourth Amendment—The Warrantless Use of Thermal Imaging Technologies Is Unconstitutional*, 71 MISS. L.J. 325, 336–39 (2001).

68. 533 U.S. 27 (2001).

a thermal-imaging device to detect heat emanating from a private home, even though they committed no trespass.[69]

Putting oneself behind closed doors creates a zone of privacy into which the police ought not intrude without a warrant. As Justice Kagan explained last year in her concurring opinion in *Florida v. Jardines*,[70] which involved the use of a drug sniffing dog, "[i]t is not surprising that in a case involving a search of a home, property concepts and privacy concepts should so align. The law of property 'naturally enough influence[s]' our 'shared social expectations' of what places should be free from governmental incursions."[71]

Smith v. Maryland need not be reversed to distinguish its application from the radically different practice of installing pen registers for everyone. Whereas *Smith* concerned a particularized search that may well be "reasonable" under the Fourth Amendment, the NSA bulk-data seizure program is the modern-day equivalent of the general warrant that strikes at the very heart of the Fourth Amendment's requirement of particularity. Both the third-party doctrine of *Smith* and the "reasonable expectation of privacy" approach of *Katz* need to be adapted to modern circumstances.

II. WHAT ABOUT THE WAR POWER AND NATIONAL SECURITY?

Some who defend the NSA surveillance programs would say that these programs should not be constrained by the Fourth and Fifth Amendments as domestic law enforcement is because they are exercises of the President's inherent power as Commander in Chief, or pursuant to the Congressional Authorization for Use of Military Force against the terrorist organizations that attacked us on September 11th. As such, the FISA procedures impose greater constraints on surveillance than was constitutionally required, even to the point of including judicial and Congressional oversight of such surveillance. Indeed, some defenders have said that it may well have been a mistake to in-

69. *Id.* at 40.

70. 133 S. Ct. 1409 (2013)

71. *Id.* at 1419 (Kagan, J., concurring) (quoting Georgia v. Randolph, 547 U.S. 103, 111 (2006)).

clude the judiciary within these procedures rather than let the President take full political responsibility for the use and abuse of such measures. This objection is a formidable one, requiring serious analysis of the scope and limits of both the President's executive power and Congress's resolution authorizing the use of military force. But let me offer some preliminary thoughts.

We can identify two legal models of constitutional powers. Call these the "domestic model" that empowers the government to protect the rights of its citizens from being violated by other members of the community; and the "wartime model" that is designed to protect the rights of American citizens from being violated by foreign enemy powers.

Constitutional protections against abuses of these powers vary. Consider that our military may kill enemy combatants in the field without any "due process of law" and may indefinitely incarcerate prisoners of war for the duration of hostilities. Neither of these measures can constitutionally be done to American citizens domestically in time of peace or war. Nor can they be done to foreign nationals in peacetime.

Those who would justify these programs under the war power are abandoning the domestic model. Therefore, any reliance on *Katz*'s "reasonable expectation of privacy" doctrine, or *Smith*'s "third-party doctrine," are make-weights and merely confuse the issue. You cannot defend the program using the "third-party" doctrine and then, when pressed on that argument, change the subject to the war power. Any war power argument must stand and fall on its own. Perhaps for this reason, in its recent brief in the ACLU's challenge to the NSA data seizures, the government did not assert the war power and never denied that the Fourth Amendment applied to this situation.

Although the government does rely on a "national security" theory of why the program is "reasonable" under the Fourth Amendment, even if it could be said to be reasonable to seize the phone records of every American in the interest of national security, this rationale cannot justify using the NSA data for domestic law enforcement purposes—as we are learning may well have occurred—or any other comparable data collection program that is used for domestic law enforcement purposes. That such mission creep has already occurred, albeit in secret, underscores the danger of allowing such bulk data seizures in the first place.

That defenders of this program will alternate between the domestic and war models of constitutional power signals that the conflict in which we are currently engaged does not fit neatly within either. The domestic model assumes that government is using its police powers to protect the rights of its citizens from others who are also members of the community. When citizens are accused of violating the rights of others that define the social compact, they deserve the benefit of the doubt before they are subjected to punishment. And we must be very careful to protect the civil liberties of the people from those in law enforcement who would abuse this police power to protect the public safety.

The war model assumes that government is using its military power to protect the rights of its citizens from threats posed by foreign powers, in particular the armies of foreign governments. Unlike persons who are accused of domestic crimes, the soldiers of a foreign power are not entitled to the protections of the Fourth and Fifth Amendments. But these war powers do not stretch into perpetuity and are typically limited to a geographically confined theater of combat. Wars between nations have both a beginning and end, and extraordinary war powers expire with the conflict that necessitated their use.

If the "cold war" between the United States and the USSR muddied the distinction between the domestic and war powers of the Congress and the President, what is sometimes called the "long war" against radical Islamic NGOs has threatened its collapse. If the battle ground is considered to include the territory of the United States, the enemy is hidden among the population, and such conflicts know no definitive end, adherence to the war power model threatens to completely subsume the protections of civil liberties afforded by the domestic model. In essence, the means of war are then turned against the People themselves to identify an enemy within.

Even if some blending of the models is warranted and that is what the original FISA and Patriot Acts were attempting to accomplish, it makes it all the more essential that the government not exceed the limits defined by these statutes. Construing Section 215 as broadly as the government now urges, and the FISA court has ruled in its secret opinions, threatens the very balance between the wartime and domestic models that Congress was presumably trying to strike. For this reason, the courts should avoid the constitutional issues by

holding that Section 215 of the PATRIOT Act does not authorize the bulk seizure of the telephone and email communications records of all Americans.

III. CONCLUSION

Let me conclude by noting that, without the recent leaks, the American public would have no idea of the existence of these programs, and it still cannot be certain of their scope.[72] Every day seems to bring new revelations about domestic surveillance by federal agencies. The secrecy of these surveillance programs is inconsistent with a republican form of government in which the citizens are the principals or masters, and those in government their agents or servants. For the people to control their servants, they must know what their servants are doing.

Moreover, until these two district courts found—over the government's objections—that citizens had standing to challenge the constitutionality of the bulk-data seizure programs,[73] their constitutionality had been assessed solely in secret by the FISC that Congress established to scrutinize the issuance of particular business record subpoenas and warrants.[74]

The secrecy of these programs, and the proceedings by which their constitutionality is being assessed, make it impossible to hold elected officials and appointed bureaucrats accountable. Internal governmental checks, and even secret congressional oversight, are no substitute for the sovereign people being the ultimate judge of their servants' conduct in office. But such judgment and control is impossible without the information that secret programs conceal.

---

72. Glenn Greenwald, *Edward Snowden: the whistleblower behind the NSA surveillance revelations*, THE GUARDIAN (June 9, 2013, 9:00 AM), http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance [http://perma.cc/542X-BMPA].

73. Klayman v. Obama, 957 F. Supp. 2d 1, 9 (D.D.C. 2013); ACLU v. Clapper, 959 F. Supp. 2d 724, 756 (S.D.N.Y. 2013).

74. *See Klayman*, 957 F. Supp. 2d at 23; Casey J. McGowan, Note, *The Relevance of Relevance: Section 215 of the USA PATRIOT Act and the NSA Metadata Collection Program*, 82 FORDHAM L. REV. 2399, 2418 (2014) ("Klayman v. Obama and ACLU v. Clapper represent the first time a non-FISC judge has weighed in on the merits of the program." (footnotes omitted)).

If these blanket seizures of privately-held data are upheld as constitutional, it would constitute an unprecedented legal and constitutional sea change. It is not a policy that should emerge from an advisory panel of judges to which the people are not privy. The American people are no longer the subjects of King George and his general warrants. Nor should we be subjected to these modern-day general warrants by those who are supposed to be our servants, not our masters.