2002

The Founders' Privacy: The Fourth Amendment and The Power of Technological Surveillance

Raymond Shih Ray Ku
Case Western University School of Law, raymond.ku@case.edu

The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance

Raymond Shih Ray Ku†

> [O]urs is a government of laws, not of men, and . . . we submit ourselves to rulers only if under rules.[1]

INTRODUCTION

A great challenge of constitutional law is to interpret a document "intended to endure for ages to come, and, consequently, to be adapted to the various crises of human affairs."[2] With respect to the Fourth Amendment[3] since the invention of the telephone, judges and scholars have debated over how to translate a document originally adopted with the investigative tools of the eighteenth century in mind to the current state of the art. For over seventy years, the tools government[4] may employ and how they may be used to combat criminals who have adopted "technological advances and used them to further their felonious purposes"[5] or simply to enforce laws more efficiently, have turned upon the Supreme Court interpretation of the Fourth Amendment and the scope of interests protected by

---

† Associate Professor of Law, Director, Institute of Law, Science & Technology, Seton Hall University School of Law. I am indebted to Susan Bandes, Erik Lillquist, Christopher Slobogin, Daniel Solove, and Charles Sullivan for their comments on an earlier draft of this Article, to the editors of the *Minnesota Law Review* for their assistance and for inviting me to participate in this symposium, and to Oded Weinstock for his capable research assistance.

1. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 646 (1952) (Jackson, J., concurring).

2. M'Culloch v. Maryland, 17 U.S. (4 Wheat.) 316, 415 (1819).

3. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . .").

4. Throughout this Article, the terms government, executive, and law enforcement are used interchangeably unless otherwise noted.

5. United States v. Scarfo, 180 F. Supp. 2d 572, 583 (D.N.J. 2001).

it. Today, the nine justices of the Supreme Court unanimously agree that privacy is the principal interest protected by the amendment. They are wrong.

The Fourth Amendment protects power not privacy. This is not to say that the Fourth Amendment has nothing to do with privacy—the amendment clearly addresses privacy, or more precisely, the right of the people to be secure. Rather, the amendment is best understood as a means of preserving the people's authority over government—the people's sovereign right to determine how and when government may intrude into the lives and influence the behavior of its citizens.[6] The amendment does so as part of the rich tapestry that is the Constitution, and cannot be viewed in isolation, but must at the very least be viewed together with the principles embodied in the constitutional separation of powers. To paraphrase Justice Jackson, the Fourth Amendment protects more than privacy; it ensures that governmental invasions of individual privacy are based upon rules established by the people, rules our rulers must follow in order to engage in surveillance.[7] Current Fourth Amendment doctrine not only ignores this principle—lost as it is in the effort to define reasonable expectations of privacy[8]—it subverts it. By limiting the Fourth Amendment's application to instances in which government invades a reasonable expectation of privacy as defined by the courts, the Supreme Court has shifted the authority for determining the scope of government's investigative power from the people to judges and law enforcement.

This power shift is accomplished by the way in which the

---

6. In this respect, the Fourth Amendment's concern for privacy is no different than its concern for law enforcement's use of force, coercion, or other methods of investigation. To the extent that Fourth Amendment law has become myopically focused on defining privacy as secrecy, I agree with William Stuntz that the focus is problematic. *See* William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1016-17 (1995). As Susan Bandes observes, the problems presented by the Supreme Court's current Fourth Amendment jurisprudence extend well beyond new technologies. Susan Bandes, *Power, Privacy and Thermal Imaging*, 86 MINN. L. REV. 1379 (2002). While this Article addresses the Supreme Court's treatment of surveillance technologies, the criticisms and suggestions raised by it are applicable to all law enforcement decisions that determine the scope of executive power, including what investigative techniques are permissible, to what weapons may be used to combat crime. A detailed discussion of all of these issues, however, is beyond the scope of this Article.

7. *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 646 (1952) (Jackson, J., concurring).

8. *See generally* Katz v. United States, 389 U.S. 347 (1967).

Court frames the Fourth Amendment inquiry. In determining whether the Fourth Amendment applies, the Supreme Court asks whether the governmental activity is considered a search under the Constitution.[9] For the most part, this inquiry loosely examines whether the government act is equivalent to the types of searches our nation's Founders considered problematic.[10] If the activity is considered equivalent then it is treated as a search, and according to the Court, the Constitution limits governmental power by imposing the requirement of a warrant supported by probable cause.[11] If the activity is not equivalent, then government agents have unfettered discretion to engage in the activity in question with no Fourth Amendment oversight or restraint. With respect to emerging technologies like the FBI's Magic Lantern project,[12] the decryption of encrypted messages,[13] or Carnivore,[14] this approach leaves open the possibility that, despite the information gathering capabilities of these technologies, their use may not be regulated at all under the Constitution because semantically, the Court may not consider their use searches.[15] As others have noted, "[t]his approach fails to protect privacy rights, and permits their gradual decay with each improved technological advance."[16]

Moreover, in engaging in this semantic game, the Supreme Court's current Fourth Amendment doctrine allows government to determine for itself the scope of its own powers. This is accomplished by assuming that law enforcement has the inher-

---

9. *See infra* Part II. For the seminal discussion of Fourth Amendment law after *Katz*, see Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349 (1974).

10. *See infra* Part II.

11. *Katz*, 389 U.S. at 357.

12. Magic Lantern is an FBI project designed to implant recording software into computers through the Internet using the same techniques and vulnerabilities exploited by hackers. *See infra* Part II.A.1.

13. Encryption is the process of converting a file into an unreadable form for the purpose of protecting the confidentiality of the content. Decryption is the process of translating the encrypted message into a comprehendible format. *See infra* Part II.A.2.

14. Carnivore is a government device programmed to capture information being delivered by an Internet service provider. *See infra* Part II.A.3.

15. *See infra* Part II.

16. Melvin Gutterman, *A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance*, 39 SYRACUSE L. REV. 647, 650 (1988); *see also* David E. Steinberg, *Making Sense of Sense-Enhanced Searches*, 74 MINN. L. REV. 563 (1990) (criticizing the incoherence of the Supreme Court's sense-enhanced search cases and suggesting three factors that may better protect Fourth Amendment privacy).

ent power to adopt and utilize new technologies subject only to narrow Fourth Amendment protections for privacy,[17] and unless a search invades a recognizable privacy interest, the amendment places no limits upon government's ability to conduct that search. In many instances this means that law enforcement, including individual officers, is not bound by any legal or constitutional restraints in deciding what surveillance devices to use, as well as when and how to use them. In the abstract, allowing the government to obtain a suspect's secret password, to decipher encoded messages, or to monitor e-mail traffic may not trouble the casual observer. After all, these tools may not only make government's job easier; in some instances they may be essential to combat technologically sophisticated criminals. When interpreting the Constitution, however, the judicial function is not to balance the relative value or efficacy of such tools against the corresponding loss of privacy and cost to society, but to determine whether the people have made such a decision either in the Constitution itself or by conferring upon their representatives the decisionmaking authority to conduct such a balancing. By leaving the decision to adopt new surveillance technologies largely to the discretion of law enforcement, the Supreme Court's current jurisprudence largely stands the amendment on its head.

Current doctrine also raises grave concerns about the fundamental relationship between the amendment and the Constitution's separation of powers. As the Supreme Court made clear in its landmark decision in *Youngstown Sheet & Tube Co. v. Sawyer*, the executive branch of government does not make the law or determine the scope of its power, but rather enforces the laws with the powers and means delegated to it by the Constitution or by statute.[18] By removing entire categories of searches from Fourth Amendment scrutiny, the Court eviscerates what is often the only limitation upon law enforcement

17. As I have discussed elsewhere, in a constitutional regime based upon the principles of popular sovereignty, assuming that government has a particular power in the process of determining whether the constitution then provides certain exceptions to those powers is a serious problem in constitutional interpretation, and is quite apparent in modern substantive due process analysis. *See generally* Raymond Ku, *Swingers: Morality Legislation and the Limits of State Police Power*, 12 ST. THOMAS L. REV. 1 (1999) (arguing that the way in which the substantive due process inquiry is framed incorrectly assumes that the power to regulate morality qua morality has been entrusted to government by the sovereign people).

18. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 587-88 (1952).

power. The absence of Fourth Amendment safeguards raises serious separation of powers concerns given that executive branch decisions to adopt and implement new surveillance technologies are often made without express legislative or constitutional authorization.[19] For the purposes of this discussion, this Article assumes that the presence of Fourth Amendment safeguards at least mitigates these concerns by placing constitutional limits upon government use of such technologies even in the absence of legislative or constitutional authorization. This assumption cannot be made, however, in the absence of Fourth Amendment protection.

All, however, is not lost. The Supreme Court's recent decision in *Kyllo v. United States*[20] may be a step in the right direction out of a jurisprudence mired in defining privacy. In deciding that the government's use of thermal imaging equipment without a warrant was unlawful, Justice Scalia concludes that when a technology is "not in general public use," the Court should "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[21] In other words, instead of asking whether the Founders would have considered the act in question a search, the Court should ask whether the Founders enjoyed this level of security from government surveillance and harassment. By grounding the analysis in the privacy enjoyed by the Founders, *Kyllo* has the potential to return the Fourth Amendment to its proper role, not because its definition of privacy is superior, but because it would subject all searches assisted by new technologies to the amendment's restraints. Taken to its logical conclusion, *Kyllo* suggests that government use of new technologies should always be subject to the warrant requirement unless they are in general public use. Consequently, law enforcement would need probable cause and a warrant before it could use technologies like Magic Lantern, decryption, or Carnivore.[22]

If the Supreme Court follows this interpretation of *Kyllo*, it would be a significant step toward reconciling the Fourth

19. My suggestion that the Fourth Amendment should be interpreted as part of the doctrine of separation of powers is similar to John Hart Ely's argument that the Fourth Amendment should be interpreted as part of the constitutional guarantee of equal protection of the laws. *See* JOHN HART ELY, DEMOCRACY AND DISTRUST: A THEORY OF JUDICIAL REVIEW 96-97, 172-73 (1980).

20. 533 U.S. 27, (2001).

21. *Id.* at 34.

22. *See infra* Part II.A.

Amendment with the doctrine of separation of powers, and returning the decision-making authority over the appropriate level of privacy and security in our society to "the people."[23] This is true in two respects. First, to the extent that the Supreme Court continues to pay lip service to its holding that a warrant is required for every search or seizure to be considered reasonable,[24] *Kyllo* keeps the already significant number of exceptions from growing even further and swallowing the rule. The "people's will" is then obeyed by adherence to their will as expressed in the Warrant Clause. Central to this interpretation is the elimination of *Kyllo's* "general public use" exception or defining the exception narrowly to ensure only the public as a whole adequately appreciates the threat of such technology and that subsequent governmental decisions to trade off privacy for effective law enforcement are made considering everyone's interests equally.[25]

Second, to the extent that this approach raises concerns that the Fourth Amendment does not require a per se warrant rule, and the Court is asked to expand its interpretation of reasonableness, which I described as the radical thesis, reasonableness should only include uses of surveillance technologies authorized by statute. In turn these statutes should be subject to judicial review to determine whether they include constitutionally adequate safeguards that substitute for a warrant. This approach would provide at least some assurance that the people rather than some of their least accountable agents determine the appropriate level of privacy and security in society and requires the Court to take seriously its representation-reinforcing role. Under this interpretation, the Fourth Amendment would permit only those uses of surveillance technologies that the people as a whole have deemed appropriate based upon the Warrant Clause, or those uses for which the people's politically accountable representatives have balanced, *ex ante*, the various privacy interests with the needs of law enforcement.

It should be apparent that this Article does not attempt to answer the riddle of when any particular search assisted by technology should be considered reasonable under the Fourth

23. U.S. CONST. pmbl.

24. *See* Katz v. United States, 389 U.S. 347, 357 (1967).

25. *See* Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, 94-95 (1988).

Amendment, which I describe as a micro-level inquiry.[26] Rather, this Article contends that we must engage in a macro-level inquiry asking the antecedent question—whether government has the power to use a particular technology to assist surveillance at all. No one questions whether law enforcement may use eyes, ears, hands, and minds to combat crime. Nor do we generally question that government should have the power to pull over vehicles that violate traffic laws, stop suspects on public streets, or break open doors. These are the tools of the physical world, and law enforcement could not function without them. With respect to these searches, the Fourth Amendment requires courts to determine whether government's focus and treatment of a particular subject was justified given the circumstances.[27] The use of emerging technologies for gathering information, however, is an altogether different inquiry. Cases evaluating the use of surveillance technologies determine the substantive level of privacy and security of society in general, not simply whether the government's investigation of a particular individual was reasonable. From Carnivore to thermal imaging,[28] the decision to allow law enforcement to use emerging surveillance technologies is effectively a decision to expand government power at the expense of the public's privacy and security. In a constitutional democracy based upon the principle of popular sovereignty, we may legitimately question the source of such power.

Part I of this Article briefly discusses the history and origins of the Fourth Amendment and its relationship to the doctrine of separation of powers. Part I argues that the central purpose of the amendment was not to define various aspects of life as private, but to guarantee that the people defined the limits of the executive's surveillance power. Part II then examines the Supreme Court's Fourth Amendment jurisprudence dealing

26. For an excellent discussion of the problems raised by *Kyllo* with respect to micro-level decisions see Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through* Kyllo's *Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393 (2002).

27. *See* William J. Stuntz, *Implicit Bargains, Government Power, and the Fourth Amendment*, 44 STAN. L. REV. 553, 553 (1992) ("In the typical Fourth Amendment case, a police officer has searched an individual or his belongings for evidence of crime. The law governing such searches is a good deal like negligence doctrine: the reasonableness of the government's action is a function of the probable gain from the intrusion weighed against the likely loss to the individual . . . .").

28. *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1475-1500 (2000) (describing various surveillance technologies).

with technology prior to *Kyllo*, and the problems associated with this jurisprudence. Part II argues that the Supreme Court's framing of the privacy question as whether a new search is equivalent to the searches the Founders feared not only fails to provide law enforcement with any guidance, but supplants the decisionmaking authority of the people in part by failing to distinguish between macro-level decisions and micro-level decisions. In this discussion, Part II uses as examples three emerging investigative technologies: Magic Lantern, decryption, and Carnivore. In Part III, this Article discusses the Supreme Court's recent decision in *Kyllo* and how it might suggest an alternative Fourth Amendment analysis based upon the Founders' privacy. This analysis is then applied to the three examples discussed in Part II. Part IV argues that unlike the Supreme Court's current approach, an analysis based upon the Founders' privacy may be consistent with the principles of constitutional self-governance and reconcile the current tension between the Fourth Amendment and the constitutional doctrine of separation of powers. Part IV.A discusses the moderate thesis, and Part IV.B the radical thesis.

I. RESPONDING TO UNBRIDLED DISCRETION AND POWER

To place the difficulties with the Supreme Court's current interpretation of the Fourth Amendment in context, a summary of the amendment's history and origins is necessary.[29] A brief review of the historical foundations of the amendment reveals that, while privacy in terms of the sanctity of home and papers was a concern prior to the amendment's adoption, the overarching concern was unfettered governmental power and discretion, and that "the people" played a prominent role in defining the scope of government power and limiting its exercise.[30] In light of this pre-constitutional history, the Fourth Amendment can be appreciated for what it is—an outgrowth and complement to the limitations placed upon executive power through the Con-

29. For more detailed discussions of the Amendment's history and origins see, for example, AKHIL REED AMAR, THE BILL OF RIGHTS: CREATION AND RECONSTRUCTION (1998); JACOB W. LANDYNSKI, SEARCH AND SEIZURE AND THE SUPREME COURT (1966); NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION (1937); William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393 (1995).

30. *See supra* note 29.

stitution's separation of powers.

A. THE FOURTH AMENDMENT AND THE FOUNDERS' CONCERNS

According to conventional wisdom, the Fourth Amendment embodies the Founders' concerns over general warrants and writs of assistance as illustrated by three pre-constitutional search and seizure cases:[31] *Wilkes v. Wood*,[32] *Entick v. Carrington*,[33] and the Writs of Assistance Case.[34] These decisions are important because of two connecting themes: concern about the privacy of an individual's home and papers against the government and fear of unbridled official power and discretion.[35] For example, the *Wilkes* case arose in response to efforts to punish John Wilkes, a well-known member of Parliament, for seditious libel as the author of a series of anonymously published pamphlets called *The North Briton*, including a pamphlet, Number 45, critical of King George III.[36] Lord Halifax, the British Secretary of State, issued a warrant that did not name Wilkes or any other individual by name, but instead, directed officials "to make strict and diligent search for the authors, printers and publishers of a seditious and treasonable paper" and "to apprehend and seize, together with their papers."[37] The officials carrying out the warrant arrested Wilkes and forty-nine other suspects by breaking into their homes and seizing their personal papers.[38]

---

31. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 463 (1928) (noting that the "wellknown historical purpose of the Fourth Amendment" was "directed against general warrants and writs of assistance"). While there is some debate over the relative importance of the writs of assistance, compare AMAR, *supra* note 29, at 66 n.* (arguing that the writ of assistance case played "very little role in the discussions leading up to the Fourth Amendment") with Tracy Maclin, *The Central Meaning of the Fourth Amendment*, 35 WM. & MARY L. REV. 197, 223-28 (1993) (arguing that the disputes over writs of assistance played an important role in colonial understanding of unreasonable searches and seizures). Because my argument does not depend upon the proper resolution of this debate, I will include the Writs of Assistance Case in this discussion. *See* Stuntz, *supra* note 29, at 396 n.9 (treating the Writs of Assistance Case as part of the Fourth Amendment canon despite this debate).

32. 19 Howell's State Trials 1153 (K.B. 1763).

33. 19 Howell's State Trials 1029 (K.B. 1765).

34. *See* M.H. SMITH, THE WRITS OF ASSISTANCE CASE (1978).

35. Stuntz, *supra* note 29, at 399-400, 406-08 (identifying the two themes connecting these cases as privacy and unbridled official discretion).

36. *Wilkes*, 19 Howell's State Trials at 1159-61.

37. The Case of John Wilkes, 19 Howell's State Trials 982, 982 (K.B. 1763).

38. Stuntz, *supra* note 29, at 399.

In response, Wilkes and several of the other suspects challenged their arrest by bringing trespass actions against the officials involved. In *Wilkes v. Wood*, Chief Justice Pratt instructed the jury that

> [t]he defendants claimed a right, under precedents, to force persons' houses, break opon escrutores, seize their papers, . . . upon a general warrant . . . , and therefore a discretionary power given to messengers to search wherever their suspicions may chance to fall. If such a power is truly invested in a secretary of state, and he can delegate this power, it certainly may affect the person and property of every man in this kingdom, and is totally subversive of the liberty of the subject.[39]

The jury found for Wilkes, awarding him one thousand pounds in damage,[40] and in a separate suit against Lord Halifax, Wilkes was awarded an additional four thousand pounds.[41] As William Stuntz notes, the cases arising out of these arrests "stand for the proposition that [general] warrants are invalid . . . and that arrests must be grounded in some cause to suspect the arrestee personally of a crime."[42] To the extent that the *Wilkes* decision influenced the Founders, it suggests that the Fourth Amendment was adopted as a means of restraining official discretion. As the Chief Justice emphasized in his jury instruction, the question raised by the case is whether anyone in government has the power to search "wherever their suspicions may chance fall."[43]

The concern over official discretion was similarly echoed with respect to writs of assistance. In the seventeenth and eighteenth centuries, British statutes gave customs officials virtually unlimited authority to search for and seize goods in violation of existing trade rules.[44] These writs of assistance did not grant the authority to search; "rather, they enabled customs officers to compel others—constables, local officials, or

39. *Wilkes*, 19 Howell's State Trials at 1167.

40. *Id.* at 1168.

41. Stuntz, *supra* note 29, at 399.

42. *Id.* at 400; *see also* Maryland v. Garrison, 480 U.S. 79, 84 (1987) (noting that the prohibition of general warrants was one of the central purposes of the Fourth Amendment); Payton v. New York, 445 U.S. 573, 583-85 (1980) (stating a similar proposition).

43. *Wilkes*, 19 Howell's State Trials at 1167.

44. For example, the Act of Frauds of 1662 authorized customs officers "to enter, and go into any House, Shop, Cellar, Warehouse or Room, or other Place, and in Case of Resistance, to break open Doors, Chests, Trunks and other Package, there to seize, and from thence to bring, any Kind of Goods or Merchandize whatsoever, prohibited and uncustomed." Act of Frauds § 5(2) (1662), *reprinted in* SMITH, *supra* note 34, at 25 (emphasis omitted).

even private citizens—to assist in carrying out the necessary searches and seizures."[45] Nonetheless, as Stuntz notes, because they permitted searches based only upon the suspicion of the customs officer, "the writs became wrapped up with the search authority they sought to confirm."[46] As another commentator observes, much like the general warrant, "[t]he odious features of writs of assistance were the unbridled discretion given public officials to choose targets of the searches," and "the arbitrary invasion of homes and offices to execute the writs."[47]

This concern over discretion was clearly a central argument in James Otis's argument against the writs. According to Otis,

> A man's house is his castle; and while he is quiet, he is as well guarded as a prince in his castle. This writ, if it should be declared legal, would totally annihilate this privilege. Custom house officers may enter our houses when they please—we are commanded to permit their entry—their menial servants may enter—may break locks, bars and every thing in their way—and whether they break through malice or revenge, no man, no court can inquire—bare suspicion without oath is sufficient.[48]

Even though Otis's argument lost, John Adams later described his argument as "the first Act of Opposition to the arbitrary Claims of Great Britain."[49] While Otis rhetorically invokes the right of privacy with his reference to the sanctity of the home, this right is clearly not absolute. The home is considered a castle only so long as the individual is "quiet" in it. This concession is quite appropriate and reasonable. Aside from questioning the validity of the underlying substantive crime, it is difficult to imagine any value that would justify an absolute right to hide evidence of a crime.[50] Accordingly, the problem with the writs was not the invasion of the castle, which is how privacy is commonly conceived, but with the process justifying

---

45. Stuntz, *supra* note 29, at 405.

46. *Id.*

47. Shirley M. Hufstedler, *Invisible Searches for Intangible Things: Regulation of Government Information Gathering*, 127 U. PA. L. REV. 1483, 1487 (1979).

48. James Otis, Address, *reprinted in* SMITH, *supra* note 34, at 344. Put another way, the writs place "the liberty of man in the hands of every petty officer." *Id.* at 331.

49. 2 LEGAL PAPERS OF JOHN ADAMS 107 (L. Kinvin Wroth & Hiller B. Zobel eds., 1965) (letter to William Tudor (March 29, 1817).

50. As Professor Stuntz has argued, *Wilkes* and *Entick* were essentially First Amendment cases in a regime in which there was not opportunity for direct substantive review. Stuntz, *supra* note 29, at 403.

the invasion. The writs gave customs officers and their "menial servants" the right to enter any home whenever they pleased. The "liberty" Otis so eloquently argued for was not an absolute right of privacy, however defined. Instead, his liberty is the liberty recognized in *Wilkes*, freedom from arbitrary and unfettered government power.

The relative importance of limiting governmental power and discretion versus defining what is private is apparent when one considers that only one of the cases in the triumvirate turned on an absolute right to keep information from the government. Like Wilkes, John Entick authored a series of pamphlets that authorities considered libelous.[51] Once again, Lord Halifax issued a warrant authorizing the Crown's agents to seize Entick and his papers.[52] Unlike *Wilkes*, this was not a general warrant because Entick was specifically named. Nonetheless, Entick sued in trespass and was awarded three hundred pounds.[53] In upholding the jury's verdict, Pratt, now Lord Camden, concluded that "[p]apers are the owner's goods and chattels: they are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection."[54] Despite the fact that the government had obtained a valid warrant, the court concluded that searching and seizing of papers themselves was impermissible. This conclusion was to be echoed in American constitutional law in *Boyd v. United States*,[55] in which the Supreme Court held that one's papers are protected by the Fourth and Fifth Amendments.[56]

While the decision in *Entick* clearly recognizes the private nature of papers, most of Pratt's decision is spent questioning the authority and process by which the warrant was issued. In affirming the trespass verdict, *Entick* rejected the power and authority of the Secretary to issue a lawful warrant as well as the lawfulness of the process by which the warrant was issued and executed.[57] Criticizing the power of the Secretary of State as "pretty singular,"[58] he rejected the idea that the Secretary of State had the power to issue warrants that could not be chal-

51. Entick v. Carrington, 19 Howell's State Trials 1029, 1031 (K.B. 1765).
52. *Id.*
53. *Id.* at 1036.
54. *Id.* at 1066.
55. 116 U.S. 616 (1886).
56. *Id.* at 634-35.
57. *Entick*, 19 Howell's State Trials at 1045.
58. *Id.*

lenged and reviewed by the judiciary,[59] or immunize its issuer and agents from subsequent prosecution.[60] According to Pratt, the laws of England did not grant the Secretary such power.[61] Instead, the Secretary's claim "stands upon a very poor foundation, being in truth no more than a conjecture of law without authority to support it."[62] Similarly, Pratt considered the warrant unlawful because, even assuming that it was supported by oath, it was executed *ex parte*, without notice or a chance to be heard, upon unknown information and informants, and its execution did not have to occur in the presence of a constable or the party.[63] These procedures were especially troubling because, if such a warrant were issued and executed against an innocent party,

> he is as destitute of remedy as the guilty: and the whole transaction is so guarded against discovery, that if the officer should be disposed to carry off a bank-bill, he may do it with impunity, since there is no man capable of proving either the taker or the thing taken.[64]

Fear of government power and discretion, therefore, runs through even the most privacy-centric decision.

It should be apparent from the Founder's concerns over general warrants and writs of assistance that a primary goal of the Fourth Amendment is the same as that of the entire Constitution—to define and limit governmental power. While the sanctity of one's home and papers,[65] as well as public disagreement with the substantive offenses,[66] clearly played an important role in these early cases, fear of unfettered governmental power resonates even more clearly. Moreover, to the extent the house and papers are to be protected, the text of the amend-

---

59. *See id.* at 1045-59.

60. *See id.* at 1059-62.

61. *See id.* at 1057 ("The whole body of the law, if I may use the phrase, were as ignorant at that time of a privy counsellor's right to commit in the case of a libel, as the whole body of privy counselors are at this day.").

62. *Id.* at 1053.

63. *Id.* at 1064-66.

64. *Id.* at 1065.

65. For example, in the Writs of Assistance Case, James Otis argued that "[a] man's house is his castle." James Otis, Address, *reprinted in* SMITH, *supra* note 34, at 344. In *Entick*, Pratt argued that "[p]apers are the owner's goods and chattels: they are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection." *Entick*, 19 Howell's State Trials at 1066.

66. *See* Stuntz, *supra* note 29, at 406-07 (arguing that the response to these decisions can be explained by public opposition to the underlying charges and offenses).

ment and its history suggest that the protection flows from restraining governmental discretion even when that discretion is specifically granted by statute. As Akhil Reed Amar suggests, the Fourth Amendment, therefore, is concerned with the agency problem, that is "protecting the people generally from self-interested government."[67] The amendment affords this protection not by defining what is private, but by expressly limiting government's power to conduct searches. Accordingly, searches must be reasonable, and warrants may only issue when supported by probable cause.[68]

For the purpose of this discussion, this history is also important because of what it suggests about how government discretion and power might be limited. While the Fourth Amendment speaks of the reasonableness of searches and the issuing of warrants except upon probable cause in the disjunctive, the Supreme Court has collapsed the two requirements, creating a general rule that warrantless searches are per se unreasonable.[69] As Part II discusses, under this approach, the Supreme Court has made itself the principal arbiter of which government acts are or are not reasonable. This interpretation of the amendment is certainly not compelled by its history and origins.[70] Instead, the Founders believed that "the people" and not judges were to "protect both individual persons and the collective people against a possibly unrepresentative and self-serving officialdom."[71]

The people exercised considerable power in these pre-constitutional cases because juries, not judges, determined the reasonableness of a search. As evidenced by *Wilkes* and *Entick*, the people would have an opportunity to evaluate searches in a common-law action for trespass. As such, "a jury, guided by a judge in a public trial and able to hear arguments from both sides of the case, could typically assess the reasonableness of government action in an after-the-fact tort suit."[72] As Amar

67. AMAR, *supra* note 29, at 67-68.

68. U.S. CONST. amend. IV.

69. *See* United States v. United States District Court, 407 U.S. 297, 315 (1972) (noting that "the definition of 'reasonableness' turns, at least in part, on the more specific commands of the Warrant Clause"); Katz v. United States, 389 U.S. 347, 357 (1967); AMAR, *supra* note 29, at 68 (noting that "[t]he modern Supreme Court has intentionally collapsed the two requirements"); Amsterdam, *supra* note 9, at 358.

70. *See* AMAR, *supra* note 29, at 64-77.

71. *Id.* at 68.

72. *Id.* at 70.

has argued in light of this background, it is not hard to imagine that "the people" were to play a similar role in restraining governmental power under the Fourth Amendment.[73] Large civil verdicts against the government agents conducting a search would deter similar behavior in the future. Moreover, once a jury concludes that the search is unreasonable, the search would be considered unlawful by definition under the Fourth Amendment.[74]

Under this regime, warrants were undesirable "pro-government" tools.[75] A lawful warrant effectively immunized the government agent from liability,[76] and removed the legality of the search from the decisionmaking authority of the civil jury.[77] Warrants, therefore, were generally disfavored and viewed with hostility, which explains why the Fourth Amendment circumscribes rather than encourages their use.[78] As Stuntz argues, this hostility stems from the fact that warrants "transferred the issue of the legality of the search from the jury . . . to a judge or executive official . . . , acting both *ex parte* and *ex ante*."[79] Hostility to warrants represented hostility to this shift in power.[80] As Amar documents in *The Bill of Rights*, throughout the ratifying debates, the Founders expressed their belief that this power was best entrusted in the people as represented by the institution of the jury rather than the judiciary.[81] As one essay at the time argued, if an officer searching

73. *Id.* ("We can now see the Fourth Amendment with new eyes.").

74. *Id.* ("If the properly instructed jury deemed the search unreasonable, the plain words of the Fourth Amendment would render the search unlawful.").

75. Stuntz, *supra* note 29, at 410 ("Warrants were a pro-government tool, not a protection for the citizenry.").

76. AMAR, *supra* note 29, at 69 ("Any lawful warrant, in effect, would compel a sort of directed verdict for the defendant government official in any subsequent lawsuit for damages."); Stuntz, *supra* note 29, at 409-10 ("A warrant provided an effective defense against a trespass claim because it established the legality of the search, creating a kind of legal 'safe harbor.'").

77. AMAR, *supra* note 29, at 69; Stuntz, *supra* note 29, at 410.

78. *See* TELFORD TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 41 (1969) ("Far from looking at the warrant as a protection against unreasonable searches, they saw it as an authority for unreasonable and oppressive searches, and sought to confine its issuance and execution in line with the stringent requirements applicable to common-law warrants for stolen goods . . . .").

79. Stuntz, *supra* note 29, at 410.

80. *Id.*

81. AMAR, *supra* note 29, at 74. As Professor Amar further notes, this also meant that state law would play a significant role in protecting individual

> for stolen goods, pulled down the clothes of a bed in which there was a woman, and searched under her shift . . . a trial by jury would be our safest resource, heavy damage would at once punish the offender, and deter others from committing the same: but what satisfaction can we expect from a lordly [judge] always ready to protect the officers of government against the weak and helpless citizen . . . ?[82]

By limiting lawful warrants to only those based upon probable cause supported by oath or affirmation, the Fourth Amendment protects the people's power to determine the lawfulness of a search.[83] By emphasizing the importance of the jury at common law, I do not intend to suggest that the jury is the only appropriate body for determining the reasonableness of a search, or even for a greater role for the jury today.[84] Judges can and must continue to play an important role in interpreting the Fourth Amendment. Rather, this discussion illustrates the importance the Founders placed on having such decisions entrusted to a popular body rather than government officials alone.

B. SEPARATION OF POWERS

One of the most perplexing problems of a government of laws and not of men is ensuring that the power wielded by the executive branch of government, "whether wielded by a Prince or a President, is itself governed by and answerable to the law."[85] Under American constitutional law, this is accomplished by requiring, at least in the domestic sphere, that executive power be governed either by the Constitution or by statute. As Laurence Tribe notes, the rejection of an all encompassing inherent executive power is dictated by the principles of popular sovereignty under constitutions that vest primary responsibility for regulating domestic activities in the legislative branch of government.[86] The executive's domestic

---

liberties. *Id.* at 76.

82. *Id.* at 74 (quoting *Essay of a Democratic Federalist*, *reprinted in* 3 THE COMPLETE ANTI-FEDERALIST 61 (Herbert J. Storing ed., 1981)).

83. U.S. CONST. amend. IV.

84. This nation and the U.S. Constitution have undergone significant changes since the eighteenth century including the rise of the professional police force, the adoption of the Fourteenth Amendment, and the fact that we are a much larger and more heterogeneous community weakening the common law jury as a safeguard.

85. 1 LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW § 4-1, at 630 (3d ed. 2000).

86. *Id.* § 4-2, at 636 ("The federal regulation of domestic affairs has its constitutional origins in the people and the states, and its initiation is allo-

role under the Constitution is best illustrated by the Supreme Court's landmark decision in *Youngstown Sheet & Tube*.[87]

In 1951, a labor dispute between steel companies and their employees threatened steel production during the Korean War. Believing that a work stoppage would jeopardize the war effort, President Truman ordered the Secretary of Commerce to take possession of and run the steel mills. The steel companies argued that the President's order violated the Constitution because it was not authorized by an act of Congress or any constitutional provision. In response, the President argued, *inter alia*, that he had the inherent power to issue such an order or at the very least that it was part of his power to "take Care that the Laws be faithfully executed."[88] Writing for the Court, Justice Black agreed with the steel companies and held that the "President's power, if any, to issue the order must stem either from an act of Congress or from the Constitution itself."[89] With respect to the President's argument that the order was consistent with his power to execute the laws, Black responded that "[i]n the framework of our Constitution, the President's power to see that the laws are faithfully executed refutes the idea that he is to be a lawmaker."[90] Instead, the Constitution limits his role to directing that "a congressional policy be executed in a manner prescribed by Congress," and the Constitution does not permit him to direct that "a presidential policy be executed in a manner prescribed by the President."[91] Because Congress did not authorize the President's actions, a majority of the Justices concluded that Truman's order was unconstitutional.[92]

In his now famous concurring opinion, Justice Jackson argued that the President claimed a power that "either has no beginning or it has no end. If it exists, it need submit to no le-

---

cated primarily to Congress. The limitation of congressional authority, and the direct electoral responsibility of Congress to the people provides some assurance to the social institutions that created the Constitution that they would not be devoured by it.").

87. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952).

88. *Id.* at 584, 587 (quoting U.S. CONST. art. II, §3).

89. *Id.* at 585.

90. *Id.* at 587.

91. *Id.* at 588.

92. In fact, when it enacted the labor laws the President claimed to be enforcing, Congress had specifically considered and rejected the idea of giving the President the power to seize striking facilities. *See id.* at 656-58 (Burton, J., concurring).

gal restraint."[93] Recognition of such a power, he argued, would be a step toward dictatorship, and was precisely what the Founders hoped to avoid by limiting the President's legislative power to recommendation and veto.[94] According to Jackson, "[w]ith all its defects, delays and inconveniences, men have discovered no technique for long preserving free government except that the Executive be under the law, and that the law be made by parliamentary deliberations."[95]

Similarly, quoting Brandeis, Justice Douglas argued,

> The doctrine of the separation of powers was adopted by the Convention of 1787, not to promote efficiency but to preclude the exercise of arbitrary power. The purpose was, not to avoid friction, but, by means of the inevitable friction incident to the distribution of the governmental powers among three departments, to save the people from autocracy.[96]

Thus, the doctrine of separation of powers protects against arbitrary and unfettered executive power by requiring executive decisions to be governed by either constitutional or statutory law.

It should be apparent that the Fourth Amendment and the doctrine of separation of powers share the same goal and are intended to serve the same function. As a complement to the doctrine of separation of powers, the Fourth Amendment may play one of two roles. Either the amendment establishes the minimum requirements that must be satisfied before government may conduct a search when those searches are authorized by statute, or it guarantees that searches are always regulated by the Constitution even if they are not specifically authorized by statute. Determining which of these roles is required by the Constitution is beyond the scope of this Article. Instead, the remainder of the discussion assumes for the sake of argument that the latter position accurately describes the relationship between the Fourth Amendment and the doctrine of separation of powers.

This brief discussion of the Fourth Amendment's history and its relationship to the Constitution's separation of powers highlights two important principles. First, the Fourth Amendment was not intended as a vehicle to define privacy;

---

93. *Id.* at 653 (Jackson, J., concurring).

94. *Id.* at 653, 655.

95. *Id.* at 655.

96. *Id.* at 629 (Douglas, J., concurring) (citing Myers v. United States, 272 U.S. 52, 293 (1926)).

rather, like the rest of the Constitution in general and the doctrine of separation of powers in particular, it is intended to limit executive power and discretion. Second, the only legitimate authority for determining the reasonableness of any exercise of governmental power is the people themselves or their legislative representatives. As Part II demonstrates, the Supreme Court either has ignored or subverted these principles when evaluating the lawfulness of technologically assisted surveillance.

II. SEARCHES THE FOUNDERS FEARED

A. TECHNOLOGY AND THE EROSION OF PRIVACY

The modern Supreme Court has responded to the challenges posed by new surveillance technologies by adopting an analytical framework that asks whether the technologically assisted search is similar to the searches the Founders feared. As Anthony Amsterdam described years ago, this approach

> proceeds from the premise that the Fourth Amendment is addressed essentially to the forcible rummagings of the English messengers and colonial customs officers. It concedes that the amendment extends to similar cases, identifies the relevant attributes of similarity, and ends by asking whether the police practice now in issue is sufficiently similar to the messengers' and customs officers' rummagings in the relevant regards.[97]

As such, the Court's approach focuses on the means employed by government, and has been described by Melvin Gutterman as the "means model"[98] or what I choose to call "means analysis." The Court's means analysis is problematic for two reasons. First, focusing on the searches the Founders feared does

97. Amsterdam, *supra* note 9, at 363.

98. Gutterman, *supra* note 16, at 650 ("Presently, the Court measures the existence of Fourth Amendment privacy solely by reference to the 'means model.'"). In contrast, at times the Court and its various justices have based their analysis on protecting the values embodied in the Fourth Amendment regardless of the means employed. *See* Olmstead v. United States, 277 U.S. 438, 478-79 (1928) (Brandeis, J., dissenting); Boyd v. United States, 116 U.S. 616 (1886); *see also Amsterdam*, *supra* note 9, at 364 ("The second approach begins by asking what concerns and judgments are implied in the decision to establish a constitutional restriction upon a category of official activity generically described as 'searches and seizures' . . . . It then inquires whether the police practice now in issue falls within the ambit of those concerns and judgments."); Gutterman, *supra* note 16, at 649 (describing a value model as one in which the Court focuses on the invasion of privacy and security and not the method for the invasion).

little to limit government discretion or to protect individual privacy and security. Instead, means analysis allows technology to drive the inquiry and erode those liberties. Second, means analysis impermissibly shifts the decisionmaking power for defining privacy and determining the appropriate level of security in society from the people to law enforcement and the judiciary.

From the beginning, the Supreme Court has taken a narrow view of the Fourth Amendment's role in limiting government discretion to employ novel technologies. In *Olmstead v. United States*, the Supreme Court concluded that the tapping of a telephone line without a warrant did not violate the Fourth Amendment.[99] Federal agents, investigating Olmstead for bootlegging, tapped his home and office telephones, recording several months' worth of conversations.[100] In determining whether the Fourth Amendment had been violated, the Court focused on the means employed by government and what those means revealed.[101] In so doing, the Court employed a simple syllogism. The Fourth Amendment speaks of searches that all involve physical intrusions and lead to the seizing of material things. The search in *Olmstead* did not require any physical intrusion or seize material things because the agents tapped into the defendants' telephones without having to trespass on private property and recorded their conversations.[102] Therefore, the Fourth Amendment does not apply to wiretapping.[103] Of course, the Court emphasized that this does not mean that privacy of telephone conversations can never be protected, only that such protection must come from Congress.[104] According to Chief Justice Taft, the searches regulated by the Constitution are only those that involve a physical trespass, and unless a search occurs, the Fourth Amendment does not apply.[105] Taft's

99. 277 U.S. at 457-66.

100. *Id.* at 455-57.

101. *See* Gutterman, *supra* note 16, at 650 (describing the Supreme Court as employing a "means" rather than a "privacy" model).

102. *Olmstead*, 277 U.S. at 464 (noting that there was no "actual entrance into the private quarters of [the] defendant" or "the taking away of something tangible. Here we have testimony only of voluntary conversations secretly overheard.").

103. *Id.*

104. *Id.* at 465-66.

105. In *Hester v. United States*, 265 U.S. 57, 59 (1924), the Court narrowed this test even further by adding the requirement that the physical intrusion take place in a protected area.

approach effectively limited the amendment's reach to only those searches that immediately concerned the Founders. To the extent that government chooses to employ new technologies that can invade individual liberty without physical intrusion, the Fourth Amendment would not stand in its way.

While the Supreme Court ultimately rejected *Olmstead's* narrow interpretation of the Fourth Amendment in *Katz v. United States*,[106] it did not tear down Taft's analytical framework. *Olmstead's* interpretation of the Fourth Amendment's reference to search and seizure as words of limitation continues to be the foundation for the Court's current doctrine. In *Katz*, the Court was asked once again to examine the validity of a wiretap. Instead of a home, however, this time the telephone tapped was a public telephone booth.[107] In holding that the amendment protects "people, not places," the Court in *Katz* adopted the general rule that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[108] Instead of determining whether government had physically intruded into a protected area, the central question would now be whether the individual had a subjectively and objectively reasonable expectation of privacy.[109] Because Katz sought to exclude the "uninvited ear" by closing the door to a public telephone booth, he was "entitled to assume that the words he utters into the mouthpiece [would] not be broadcast to the world."[110] How the government defeated that expectation was irrelevant. Because the wiretapping of the telephone booth was not authorized by "the deliberate, impartial judgment of a judicial officer," it violated the Fourth Amendment.[111]

While abandoning *Olmstead's* narrow focus on physical intrusions, the *Katz* analysis maintains *Olmstead's* focus on de-

106. 389 U.S. 347, 353 (1967) ("Once it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.").

107. *Id.* at 348.

108. *Id.* at 351-52 (citations omitted).

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

110. *Id.* at 352.

111. *Id.* at 357 (quoting Wong Sun v. United States, 371 U.S. 471, 481-82 (1963)).

termining whether government conduct should be considered a search. If the information is exposed to the public, gathering of that information is not a search and the Fourth Amendment does not apply. If the information is private, then government gathering of that information is a search requiring a warrant or consent.[112] *Katz*, therefore, does not reject the *Olmstead* inquiry so much as it expands the scope of that inquiry. Melvin Gutterman has argued that *Katz* went further, "declaring that a privacy value-oriented analysis should replace" the *Olmstead* approach.[113] Standing alone, I would agree with Gutterman that logically *Katz* should be interpreted as employing an analysis focused on determining privacy values rather than examining the means employed by government.

> The entire thrust of the [Katz] opinion is that it is needless to ask successively whether an individual has the kind of interest that the fourth amendment protects and whether that interest is invaded by a kind of governmental activity characterizable by its attributes as a "search." Rather, a "search" is anything that invades interests protected by the amendment.[114]

However, by failing to provide any real guidance or substance to the privacy value, the opinion did not shut the door to examining means, and subsequent decisions have taken advantage of this opening, artfully transforming the reasonable expectation of privacy test into a means-oriented analysis.[115] Accordingly, "[a]s long as the manner of acquiring the information could be squeezed into the Katz terminology, the nature of the privacy value implicated need only be minimally examined."[116] As Amsterdam recognized, simply by substituting the phrase "government intrusion" for the finding that the government had "violated" Katz's interests creates the "subtle suggestion that a particular kind or sort of government activity, labeled an 'intrusion,' is necessary to trigger the [F]ourth [A]mendment."[117] Regardless of what *Katz* originally intended,

---

112. *Id.* at 353.

113. Gutterman, *supra* note 16, at 662.

114. Amsterdam, *supra* note 9, at 383.

115. *See* United States v. Karo, 468 U.S. 705, 712 (1984) ("A 'search' occurs 'when an expectation of privacy that society is prepared to consider reasonable is infringed.'") (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984)); *see also* Kyllo v. United States, 533 U.S. 27, 31-33 (2001) (describing the Court's means analysis); Dow Chem. Co. v. United States, 476 U.S. 227, 237-38 (1986) (focusing on the manner of surveillance to determine that the taking of aerial photographs was not a search).

116. Gutterman, *supra* note 16, at 711.

117. Amsterdam, *supra* note 9, at 383.

if *Olmstead* interpreted the Fourth Amendment's reference to searches as limited only to those searches the Founders feared, *Katz* and its progeny now interpret the Amendment as applying only to searches analogous to those the Founders feared.

Since *Katz*, a multitude of factors are considered to determine whether new technologies are similar to the searches the Founders feared.[118] These factors include 1) the nature of the place to be observed; 2) the ease of observation; 3) the location of the observer, including whether surveillance requires physical intrusion; 4) the nature of the object or activity observed; 5) the availability of the technology to the general public; 6) whether the technology enhances natural senses; and 7) the duration and scope of the surveillance.[119] These factors are non-exclusive, with some weightier than others, and as the following discussion illustrates arguably the first and third are the most important for technologically enhanced searches.[120]

Consider the Supreme Court's decisions in *United States v. Knotts*[121] and *United States v. Karo*[122] in which the Court considered whether using electronic tracking devices constituted a search under the Fourth Amendment. In *Knotts*, the police placed a "beeper" or radio transmitter in a five-gallon drum of chloroform.[123] Using the beeper, they were able to track the drum from its place of purchase in Minnesota to the Knotts' cabin in Wisconsin in which they discovered a drug laboratory.[124] In upholding the warrantless use of the beeper, the Supreme Court concluded that the information provided by the beeper was no different than what the officers could have ob-

118. *See* Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*, 10 HARV. J. L. & TECH. 383, 390-404 (1997) (summarizing the factors from the case law); Steinberg, *supra* note 16, at 583-605 (arguing that the Supreme Court should consider 1) physical trespass; 2) the visual/aural distinction; 3) plain view analogies; and 4) implicit consent).

119. Slobogin, *supra* note 118, at 390-98.

120. Some commentators have suggested that practically speaking, the Supreme Court is simply determining whether the search in question was reasonable. *See* Craig M. Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1484-85 (1985) (arguing that in many circumstances, the Supreme Court is simply evaluating the reasonableness of the search); Stuntz, *supra* note 27, at 557-62 (arguing that in the ordinary criminal case Fourth Amendment law is analogous to the law of negligence).

121. 460 U.S. 276 (1983).

122. 468 U.S. 705 (1984).

123. 460 U.S. at 277.

124. *Id.* at 277-79.

served visually.[125] Accordingly, "[n]othing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case."[126] In contrast, government agents in *Karo* used a beeper to track fifty gallons of ether not only on public roads, but also to locate the ether within specific residences.[127] The Court began by describing private residences as "places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant."[128] It then held that monitoring of the beeper within private residences violated the Fourth Amendment, because it allowed the government to "obtain information that it could not have obtained by observation from outside the curtilage of the house."[129]

While outwardly these decisions follow *Katz*, they do so only formalistically. Noticeably absent is any real effort to evaluate whether electronic surveillance should be considered the equivalent of visual surveillance or why a residence should be treated differently than a moving vehicle. Practically, these decisions would allow government to monitor any individual outside of the home twenty-four hours a day without any discussion of how that monitoring might affect the individual or what that surveillance might do to the relationship between government and individual.[130] As Justice Brennan argued in another case, technologically enhanced surveillance is "more penetrating, more indiscriminate, more truly obnoxious to a free society. Electronic surveillance, in fact, makes the police omniscient; and police omniscience is one of the most effective tools of tyranny."[131] Instead, *Knotts* and *Karo* mechanically apply *Katz's* statement that government surveillance of what an individual exposes to the public is not a search.[132]

---

125. *Id.* at 282.

126. *Id.*

127. 468 U.S. at 708.

128. *Id.* at 714.

129. *Id.* at 715.

130. Gutterman, *supra* note 16, at 705.

131. Lopez v. United States, 373 U.S. 427, 466 (1963) (Brennan, J., dissenting).

132. In substance and spirit, *Knotts* and *Karo* are also closer to *Olmstead* than *Katz*. By recognizing a significant distinction between the public roads and private residences, these decisions effectively resurrect *Olmstead's* reliance upon property interests. This trend in the doctrine is even more apparent in the Court's decisions involving overflights. *See* California v. Ciraolo,

Another illustration of the means approach and its formalistic reliance on "public exposure" can be found in *Smith v. Maryland*.[133] In *Smith*, a victim of a robbery received threatening and obscene telephone calls from an individual identifying himself as the robber.[134] When police subsequently identified Smith as fitting the robber's description, they had the telephone company install a pen register to record the phone numbers dialed by Smith.[135] The register revealed that Smith subsequently called the victim.[136] In holding that the use of the pen register was not a search, the Court concluded that Smith could have had no reasonable expectation of privacy in the numbers he dialed because his use of the phone "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business."[137] Not only was the information collected by the pen registry more limited than that collected by wiretaps, it did not divulge the contents of the communication.[138] Having thus exposed this information, the Court concluded that Smith "assumed the risk" that the telephone company might turn this information over to the police.[139] The Court reached this conclusion by assuming away rather than examining the privacy values at stake.

While not high technology, government use of drug-sniffing canines highlights some of the other factors considered in determining whether a search has occurred. These factors have clear implications for government use of technological tools. In

476 U.S. 207, 213 (1986) (holding that visual surveillance of a homeowner's backyard was not a search despite the existence of a ten foot fence enclosing the backyard); Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986) (holding that the use of a commercial mapping camera from an airplane was not a search). These decisions effectively hold that, because the areas under surveillance were visible to the flying public and because the police did not trespass to obtain the information but instead conducted their surveillance from a publicly accessible vantage point, the Fourth Amendment does not apply.

133. 442 U.S. 735 (1979).

134. *Id.* at 737.

135. *Id.*

136. *Id.*

137. *Id.* at 744.

138. *Id.* at 741 (noting that a pen register "differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications.").

139. *Id.* at 744.

United States v. Place,[140] the Supreme Court held that use of a highly trained dog to sniff for narcotics was not a search governed by the Fourth Amendment.[141] In arriving at this conclusion, the Court characterized the dog sniff as much less intrusive than a typical search because it does not require the opening of luggage or the exposure of non-contraband items.[142] Moreover, the information gathered is limited; the canine sniff determines only whether narcotics are present.[143] According to the Court, the focused and limited nature of this inquiry "ensures that the owner of the property is not subjected to the embarrassment and inconvenience entailed in less discriminate and more intrusive investigative methods."[144] While the Court opined that dog sniffs are *sui generis*,[145] *Place* can be used to exempt technologically assisted searches as well.

As the foregoing decisions demonstrate, in determining whether the Fourth Amendment regulates government searches, the Supreme Court asks whether a particular search is similar to those the Founders feared. It should be apparent that by focusing on the means employed by government in conducting its investigation, this approach allows technology to dictate the degree of privacy and security that society will enjoy. To the extent that surveillance tools like beepers, pen registers, and drug-sniffing dogs do not raise the same or similar privacy concerns as rummaging by colonial customs officers, the Fourth Amendment does not apply. As illustrated by the following three examples, new technologies are likely to erode privacy even further.

1. Net-Wide Searches and Magic Lanterns

Today, more and more individuals own or use computers connected with one another through the Internet. Suppose the FBI created a program to scour all of these computers for specific files such as child pornography or copyright infringing mp3s.[146] If the program finds the specified file, it notifies the FBI that the information has been found and where it is lo-

140. 462 U.S. 696 (1983).
141. *Id.* at 707 (1983).
142. *Id.*
143. *Id.*
144. *Id.*
145. *Id.*
146. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 17 (1999).

cated. If it finds nothing, the program erases itself. This program would not interfere with computer operations or functionalities. The owner of the computer would not even know it was there. Would the use of the program represent a search subject to the Fourth Amendment?

When originally popularized by Lawrence Lessig, this "net-wide search" was merely hypothetical. Today, it is one step closer to reality. Toward the end of 2001, the FBI confirmed that it was developing an Internet surveillance program code-named "Magic Lantern."[147] Magic Lantern would allow the FBI to install a program that records every keystroke on a person's computer without the need to physically access the computer.[148] The FBI would accomplish this by using many of the same techniques and exploiting many of the same weaknesses in commercial software that hackers use for delivering viruses across the Internet.[149] Magic Lantern and its predecessor, the "Key Logger System," have been designed to respond to the criminal and terrorist use of encryption to scramble *messages* and computer files.[150] Recently, a U.S. District Court upheld the FBI's use of the key logger system to obtain information needed to read the computer files of an accused organized crime figure who used a popular encryption program.[151]

Arguably, especially to the uninitiated, the net-wide search and Magic Lantern should run afoul of the Fourth Amendment in the absence of a warrant. After all, a net-wide search could be considered the cyber-equivalent of a general warrant, both of them gathering information that individuals endeavor to keep secret, and both in some sense acts of trespass.[152] Both also give government unfettered discretion to intrude into an indi-

147. *See* Ted Bridis, *FBI Develops Eavesdropping Tools*, AP ONLINE, Nov. 22, 2001, WL 30247847; *FBI Confirms MSNBC.COM Story on "Magic Lantern,"* BUS. WIRE, Dec, 13, 2001, WL 12/13/01 Bus. Wire (reporting in both wire service items the existence of Magic Lantern and describing the program).

148. Bridis, *supra* note 147.

149. *See id.*

150. *Cf. id.* (explaining problems with using the "Key Logger System," which mandated a "sneak-and-peak warrant" to "attach" a "device to a computer."). For a definition of encryption see *infra* text accompanying note 157.

151. *See* John P. Martin, *FBI Upheld on Use of Cyber-Snoop*, STAR LEDGER, Dec. 27, 2001, at 21.

152. *See, e.g.*, eBay v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1069 (N.D. Cal. 2000) (holding that a claim of trespass to computers is legally cognizable); Compuserve Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1023-24 (S.D. Ohio 1997) (recognizing a claim of trespass to computers).

vidual's computer without any evidence that the individual has committed any wrongdoing. Under the Supreme Court's current doctrine, however, it is possible for a court to conclude that the Fourth Amendment does not govern the FBI's use of these technologies at all. Assuming that these programs are designed to capture only a limited amount of information or only contraband information,[153] they would appear to be the cyber-equivalent of the dog sniff in *Place*.[154] These searches are less intrusive than physical searches—they gather only limited information, and they minimize embarrassment and inconvenience. Moreover, to the extent that some members of the public (i.e., hackers) may access the same information through the Internet, a court may conclude that the information is not private because individuals assume the risk that others, including the government, may access this information once a computer is connected to the Internet.[155]

2. Encryption/Decryption

In an age in which significant amounts of information are both transmitted and stored electronically, to what extent should the use of encryption establish a reasonable expectation of privacy? More specifically, must the government obtain a warrant before it can decrypt an encrypted file? The importance of these questions cannot be overstated. As Judge Fletcher recognized,

> Whether we are surveilled by our government, by criminals, or by our neighbors, it is fair to say that never has our ability to shield our affairs from prying eyes been at such a low ebb. The availability and use of secure encryption may offer an opportunity to reclaim some portion of the privacy we have lost. Government efforts to control encryption thus may well implicate not only the First Amendment rights of cryptographers intent on pushing the boundaries of their science, but also the constitutional rights of each of us as potential re-

153. This is a fairly significant assumption, and was one of the key issues in the Scarfo investigation. The FBI refused to disclose how the key logger system functions, and the district court ultimately concluded that the defendant was only entitled to a summary of how the program functioned. *See* United States v. Scarfo, 180 F. Supp. 2d 572, 580-81 (D.N.J. 2001); Martin, *supra* note 151, at 21.

154. *See supra* text accompanying notes 141-42.

155. *See* United States v. Hambrick, 55 F. Supp. 2d 504, 508-09 (W.D. Va. 1999) (concluding that individuals have no reasonable expectations of privacy in their Internet IP addresses because those addresses are voluntarily exposed to others).

cipients of encryption's bounty.[156]

In brief, encryption is the process of running a readable plaintext message through a computer program that translates the message according to an equation or algorithm into an unreadable ciphertext. Decryption is the process of translating the ciphertext back to plaintext, which is usually accomplished by the use of an encryption key.[157] Magic Lantern is designed to enable government to obtain encryption keys, but because encryption is based upon an algorithm, it is possible to break the encryption and decrypt the message without the key either by figuring out the algorithm, and then translating the message oneself, or by randomly entering information until that information matches the key.[158] For example, pig Latin is a simple form of encryption in which English words are rearranged and additional syllables added according to a predetermined set of rules. It is possible of course to break or decrypt a message in pig Latin simply by determining what the rules are or by rearranging the words and syllables at random until they become a coherent message. State of the art encryption, however, is much more difficult to break.[159] To the extent that it is even possible, breaking sophisticated encryption requires the use of supercomputers, and even those computers might take years to unscramble the information.[160]

At first glance, by rendering electronic messages undecipherable, encryption would appear to create a reasonable expectation of privacy because it could be the digital equivalent of sealing correspondence in an envelope. In fact, the term envelope is regularly used to describe the encryption of messages.[161]

---

156. Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1146 (9th Cir. 1999), *withdrawn*, 192 F.3d 1308, 1309 (1999).

157. Bernstein v. U.S. Dep't of State, 974 F. Supp. 1288, 1292 (N.D. Cal. 1997), *aff'd* Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132 (9th Cir. 1999), *rehearing granted, opinion withdrawn* Bernstein v. U.S. Dep't of Justice, 192 F.3d 1308 (9th Cir. 1999).

158. Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy"?*, 33 CONN. L. REV. 503, 529-30 (2001) (noting that since "an encryption 'key' is really just a string of 0's and 1's, decryption programs generally work by trying every possible combination until the right key happens to be found (so-called 'brute force' methods)").

159. *Cf. id.* at 503.

160. *See id.* ("Because encryption keys are in most cases impossible to guess—trying to guess a single key could occupy a supercomputer for millions of years—encryption offers Internet users a degree of privacy in Internet communications that remains unequaled in the physical world.").

161. *Cf.* Lee Tien, *Publishing Software as a Speech Act*, 15 BERKELEY

If encryption were considered the equivalent of using a sealed envelope, then it would appear that the Supreme Court would require the government to obtain a warrant before it could decrypt messages either through the use of a key or by breaking the encryption.[162] After all, individuals have a reasonable expectation of privacy in sealed envelopes, and opening sealed envelopes is considered a search.[163]

Once again, though, the Supreme Court's current doctrine leaves room for doubt. Relying upon the concepts of public exposure and assumption of risk, Orin Kerr has argued that government efforts to decrypt messages should not be considered searches under the Fourth Amendment.[164] According to Kerr, once the government obtains an encrypted message, the message itself is effectively "in plain view."[165] Encryption, therefore, merely affects the government's ability to understand the message, not to access it.[166] As such, he argues that when "the government obtains communications in a form that it does not understand, the Fourth Amendment does not require law enforcement to obtain a warrant before translating the documents into understandable English."[167] In other words, government decryption of a message is no different than the government's translation of Spanish into English,[168] which is not considered a search under the Constitution.[169]

TECH. L.J. 629, 672 (2000) (drawing an analogy between "envelopes for written correspondence" and encryption).

162. *See* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 871 (1995) (arguing that encryption "is armor around a communication much like a safe is armor around a possession. A person who puts something in a safe to which they have the only key or combination surely has both a subjective and objective reasonable expectation of privacy.").

163. *See Ex parte* Jackson, 96 U.S. 727, 727 (1877); United States v. Robinson, 414 U.S. 218, 248 (1973) (Marshall, J., dissenting).

164. Kerr, *supra* note 158, at 505; *see also* Note, *Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 110 HARV. L. REV. 1591, 1604 (1997) ("Unlike a communication hidden by a password, an encrypted message can still be viewed, albeit in encoded form . . . . [T]he encoded message, once observed, may be decoded without implicating the Fourth Amendment . . . .").

165. Kerr, *supra* note 158, at 520.

166. *See id.* at 517-20.

167. *Id.* at 518.

168. *See id.*

169. *See* United States v. Langoria, 177 F.3d 1179, 1183 (10th Cir. 1999) (holding that a defendant who spoke in Spanish had no reasonable expectation of privacy that the communication would not be translated because he know-

3. Carnivore

Lastly, consider the government's program DCS1000—otherwise known as "Carnivore." Carnivore is a device capable of collecting and monitoring all online activities from e-mail to web surfing at a particular Internet service provider (ISP).[170] According to the FBI, Carnivore would be configured so that it could return certain sought-after information.[171] It would accomplish this by capturing all of the information that passes through an ISP, and then extracting only the sought-after information.[172] For example, if the FBI sought to determine with whom a particular individual was corresponding via e-mail, Carnivore could be configured to "filter out" all other information, including the content of that individual's e-mail.[173] While it would chew all the information that came through the Internet, it would only digest the sought-after information. Carnivore, therefore, can be programmed to limit the information viewed by human eyes.[174] In many respects, Carnivore is the mirror image of the net-wide search. Instead of "going out" onto the net to search for information, however, the device collects information as it passes through one of the Internet's many gateways. Like an information roadblock, it screens all traffic, but pulls over only the data packets it has been programmed to capture.

Despite the fact that Carnivore effectively collects all of the information going through an ISP and searches that information, an argument can be made that the government would not need a warrant or court order to unleash Carnivore.[175] *Smith* suggests that because an Internet user knowingly exposes information to her ISP, she assumes the risk that the ISP may

---

ingly exposed his communication to others and assumed the risk that it would be translated).

170. *See* Donald M. Kerr, Lab. Div., Fed. Bureau of Investigation, *Carnivore Diagnostic Tool*, Statement for the Record, United States Senate, Committee on the Judiciary (Sept. 6, 2000), *available at* http://www.fbi.gov/congress/congress00/kerr090600.htm.

171. *Id.*

172. *Id.*

173. *See id.*

174. *See id.*

175. This assumes that Carnivore does not report the contents of e-mails or online aural communications, which would be arguably governed by *Katz* and the wire tape provisions of the Electronic Communications Privacy Act. *See* Katz v. United States, 389 U.S. 347, 357 (1967).

turn this information over to the government.[176] If Carnivore is programmed, for example, to capture the addresses of people with whom an individual is corresponding via e-mail, the analogy to *Smith* and the capturing of telephone numbers is even closer. *Knotts* could also be used to exempt the tracking of an individual's online activities.[177] The individual exposes her web viewing habits to more than just her ISP; they are exposed to the various websites someone visits, the companies that gather this information for marketing purposes, and potential hackers as well. Arguably, web surfing is much like driving on the public streets. Likewise, *Place* could be relied upon because even though Carnivore searches all of the information at an ISP, unless it is the sought-after information, it is not viewed by human eyes, thus minimizing intrusion, embarrassment, and inconvenience.[178] It is possible, therefore, to argue that Carnivore is not similar enough to the searches the Founders feared.

As these cases and examples illustrate, as technology becomes more powerful and capable of gathering information without trespassing or opening locked doors and drawers, current Fourth Amendment law suggests that the use of surveillance technology is not a search. Whether one agrees with the results of the preceding cases or examples will depend a great deal on how one defines privacy and how one balances the needs of law enforcement against individual security. Whatever one may think about the merits, by limiting the Fourth Amendment to only those searches that are sufficiently similar to those the Founders feared, the Supreme Court has allowed technology to diminish the level of privacy and security we can expect in society. While this should certainly be of some concern to all of us, it is not the most troubling consequence of the Court's current approach. Debating over the definition of privacy and whether or not a particular search invades such a right distracts us from the fundamental power shift that has occurred under the current interpretation of the amendment.

176. *See* United States v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999) (finding no reasonable expectation of privacy in subscriber information).

177. United States v. Knotts, 460 U.S. 276, 281 (1983) (using as an analogy the fact that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another").

178. *See supra* text accompanying note 141.

B. DISCRETION AND POWER

Under the Supreme Court's current interpretation of the Fourth Amendment, the Constitution plays only a small role in restraining government power, and the people play virtually no role in defining the scope of that power. The irony is, of course, that what the Founders feared was not the invasion of privacy per se, but how and when those invasions would occur. As Part I discussed, the Founders were more concerned about limiting government's power to invade any aspect of life without sufficient cause than with defining what aspects of life should be off limits to government. The Founders also believed that the people should play a significant role in making this determination. The Supreme Court's current approach does more than ignore these concerns—it undermines them. As it stands, the Supreme Court has transformed the Fourth Amendment from a constitutional provision delineating the scope of governmental power generally as determined by the people into a provision that protects only isolated pockets of interests as determined by judges.

According to the Supreme Court, the Fourth Amendment establishes a general rule that for a search to be considered reasonable it must be authorized by warrant.[179] Although the Court has never seriously questioned this rule, it has spent over a quarter of a century creating exceptions to it.[180] And, "reading a warrant requirement into the amendment, and then reading an elaborate set of exceptions into that warrant requirement, seems more like rewriting the amendment than reading it as written."[181] The Court has accomplished this feat, as Justice Black noted, by "clever word juggling."[182] Seizing upon the concept of privacy as secrecy despite the fact that *Katz* itself recognized that the amendment "cannot be translated into a general constitutional 'right to privacy,'" and that "its protections go further,"[183] later Courts have narrowly defined what constitutes a search for the purposes of the Fourth Amendment—categorically excluding certain government acts from constitutional scrutiny.[184]

---

179. *Katz*, 389 U.S. at 357.

180. *See* California v. Acevedo, 500 U.S. 565, 582-83 (1991) (Scalia, J., concurring) (discussing twenty-two exceptions to the warrant requirement).

181. AMAR, *supra* note 29, at 68-69.

182. *Katz*, 389 U.S. at 373 (Black, J., dissenting).

183. *Id.* at 350.

184. *See supra* Part II.A.

In contrast, in his now famous dissent in *Olmstead*, Justice Brandeis took issue with what he perceived as the Court's "unduly literal" interpretation of the amendment. According to Brandeis,

> When the Fourth and Fifth Amendments were adopted, "the form that evil had theretofore taken," had been necessarily simple. Force and violence were then the only means known to man by which a government could directly effect self-incrimination. It could compel the individual to testify—a compulsion effected, if need be, by torture. It could secure possession of his papers and other articles incident to his private life—a seizure effected, if need be, by breaking and entry . . . . But "time works changes, brings into existence new conditions and purposes." Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.[185]

The protection afforded by the Constitution for individual liberties must, Brandeis argued, change to meet the problems of the day.[186] Because technology will continue to develop new and even more powerful means for gathering information, the Court should guarantee the "right to be let alone," the right of Americans to be secure not only in their physical possessions, but also "in their beliefs, their thoughts, their emotions and their sensations."[187] As such, Brandeis rejected means analysis, and argued that the protections guaranteed by the Constitution are much broader in scope. Instead of preventing only those invasions of liberty sufficiently similar to what the Founders feared, the Court's role should be to protect individuals from all intrusions into the right to be let alone.[188] Because wiretapping violated this liberty and was arguably an even greater invasion than more traditional searches and seizures, he considered the government's actions unlawful under the Fourth Amendment.[189]

Except on the rare occasions when the Supreme Court recognizes a search as a search, the determination of whether government may use technology to engage in surveillance and how to use that technology is left entirely to the discretion of law enforcement. The people play almost no role in determining the

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

186. *See id.* at 472.

187. *Id.* at 478.

188. *See id.*

189. *See id.* at 475-79.

scope of government's power or whether any particular exercise of that power is reasonable. Either the Supreme Court considers the use of technology a search requiring a warrant, or the government's use of the technology is absolutely unrestrained by the Constitution.[190] In so doing, the Court has interpreted the Fourth Amendment to vest the authority to determine the appropriate level of privacy and security in this nation in an institution whose power the Founders sought to restrain. The Justices certainly have "stood the [F]ourth [A]mendment on its head."[191]

Consider once again the Court's decision in *Olmstead*. Often overshadowed by the debate between Taft and Brandeis over how to define privacy is their exchange over the role of the underlying state law. In *Olmstead*, a state law prohibited wiretapping.[192] The federal officers, however, obtained the evidence against Olmstead by violating that state law. Taft treated this fact as irrelevant for purposes of Fourth Amendment analysis, and merely concluded that, under the common law, evidence is admissible even if illegally obtained.[193] In contrast, both Brandeis and Holmes believed that the prosecution should not have been allowed to continue precisely because of the government's misconduct.[194] Both Justices were concerned with this abuse "on behalf of the United States,"[195] and believed that the evidence should have been excluded,[196] but neither considered state law relevant in determining the reasonableness of the search under the Fourth Amendment. Brandeis argued that the case should be dismissed as a matter of equity,[197] while Holmes argued that the exclusionary rule should be applied to violations of law in addition to violations of the Constitution.[198] In light of the role that common-law trespass played in this re-

190. *See* Amsterdam, *supra* note 9, at 388 ("On the other hand, if it is not labeled a "search" or "seizure," it is subject to no significant restriction of any kind.").

191. *See* TAYLOR, *supra* note 78, at 23-24.

192. *See Olmstead*, 277 U.S. at 469.

193. *See id.* at 467-68.

194. *See id.* at 480 (Brandeis, J., dissenting); *id.* at 469-70 (Holmes, J., dissenting).

195. *Id.* at 483 (Brandeis, J., dissenting).

196. *Id.* at 480 (Brandeis, J., dissenting); *see id.* at 469-70 (Holmes, J., dissenting).

197. *See id.* at 483-84 (Brandeis, J., dissenting).

198. *See id.* at 469-70 (Holmes, J., dissenting).

gard,[199] the omission is particularly troublesome because it ignores the role that both federalism and the people play in controlling governmental discretion and safeguarding individual liberty under the amendment.[200] This is not to suggest that state law or federal statutes are the only or preferred means of protecting individual liberty, but rather that courts should not ignore the important role legislatures play in our tripartite government in determining the appropriate amount of power to be exercised by law enforcement. Laws prohibiting certain forms or means of information gathering, therefore, should limit executive power and define at least minimum levels of privacy and security protected by the Fourth Amendment.[201]

In defense of the Justices, the adoption of this interpretive framework may well be explained as recognition that the police require significant discretion at what I will call the micro level—how best to exercise power in a particular situation or to capture a particular criminal. The police constantly deal with danger and the unknown, and they must have the power to protect themselves as well as the public in highly fluid situations. Likewise, through their unique experiences, officers may develop special expertise and judgment, and society is better off when experienced officers are allowed to follow their hunches and target suspects to prevent a crime from occurring or to capture them after the fact. So when a suspect uses encryption to hide her computer files, it is generally up to the police to determine the best way to obtain that evidence, whether it be by breaking into the computer and physically implanting a key logger, using Magic Lantern over the Internet, or convincing an accomplice to copy the files. Given that the Supreme Court decides individual cases in which law enforcement's exercise of micro-level discretion actually uncovered evidence of a crime and led to the capture of the perpetrator, it would be difficult to conclude that the exercise of that discretion was unreasonable

199. *See supra* Part I.

200. AMAR, *supra* note 29, at 76 ("Vindication of [Fourth Amendment] restrictions would largely come from state bodies. State statutes and state common law, after all, would typically define and protect ordinary individuals' property rights to their 'persons, houses, papers, and effects.' Thus state law would initially create the trespass cause of action that would enable ordinary men and women to challenge unconstitutional intrusions by federal officials." (quoting U.S. CONST. amend. IV)).

201. Of course, unless passed by Congress, laws prohibiting the use of surveillance technologies will vary from state to state, leaving open the possibility that individual liberties will vary as well.

unless it led to discriminatory harassment of individuals or selective enforcement of the law.

However, we should not confuse police decisionmaking at the micro level with macro level decisions that determine the scope of executive power in general. While the Constitution may permit a degree of deference at the micro level, it leaves little room at the macro level. The decision to adopt a new form of surveillance technology is just such a macro-level decision. The decision to adopt Magic Lantern or Carnivore is a determination to expand the powers and capabilities of the executive branch and correspondingly to reduce the level of privacy and security individuals may expect and enjoy. Whatever deference law enforcement may be entitled to with respect to micro level discretion, it is entitled to none at the macro level. Unfortunately, the Court's current Fourth Amendment jurisprudence virtually ignores the distinction between micro and macro-level decisionmaking, and never questions from where law enforcement derives its authority to adopt these new technologies.

The Supreme Court's failure to question the source of law enforcement's power to adopt new technologies leads to a significant incongruity. The individual officer, a relatively low member of the executive branch, in many respects, has more discretionary power than the President. Unlike the President, whose power in general must be granted either directly by the Constitution or by acts of Congress,[202] many of the activities the police engage in are not authorized by law at all, but are instead conducted under "their broad general duties to enforce the law and keep the peace."[203] While the Supreme Court carefully scrutinizes presidential claims of inherent authority, it appears to assume the President's inherent authority when law enforcement is concerned.[204] In this respect, the Supreme

202. *See supra* Part I.B.

203. Amsterdam, *supra* note 9, at 386; *see also* Dow Chem. Co. v. United States, 476 U.S. 227, 233 (1986) ("Regulatory or enforcement authority generally carries with it all the modes of inquiry and investigation traditionally employed or useful to execute the authority granted.").

204. One might argue that this assumption is warranted because state constitutions do not follow the same doctrine of separation of powers as the U.S. Constitution. While one can argue that state legislative power is broader than congressional legislative power, there is no support for the argument that the doctrine of separation of powers with respect to state executive power differs from the federal doctrine. As even a critic of this approach recognizes, "federal precedent sets the terms for much state separation of powers debate, and federal principles provide a presumptive standard for state constitutional decisions." Robert A. Shapiro, *Contingency and Universalism in State Separa-*

Court's Fourth Amendment jurisprudence must learn from its evaluation of presidential power in the *Steel Seizure Case*. Unless the people grant the executive branch the power in question either through the Constitution or through legislation, claims of inherent executive power are suspect.[205] As it stands, under the Court's current approach, the people play absolutely no role in determining the extent and reasonableness of government's power to search. Instead, the Court treats law enforcement as having unfettered government power to invade individual privacy and security subject only to a few not so well defined but limited exceptions defined by the Court. Whatever role the Fourth Amendment might have played in regulating executive power consistently with the doctrine of separation of powers, in many instances it currently plays no role whatsoever. This state of affairs is precisely what the Founders feared most.

III. A HEAT SOURCE AT THE END OF THE TUNNEL?

The Supreme Court's most recent Fourth Amendment decision involving new technology may be the first step in preventing the "power of technology to shrink the realm of guaranteed privacy,"[206] and restoring the Fourth Amendment to its intended role of preserving the people's authority to limit unfettered government power. *Kyllo v. United States* arguably re-

---

tion of Powers Discourse, 4 ROGER WILLIAMS U. L. REV. 79, 80 (1998); *see also* People v. Moore, 102 N.E.2d 146, 151-52 (Ill. 1951) (recognizing that the doctrine of separation of powers only permitted the police to seize items specifically defined by state statute); Ronald J. Allen, *The Police and Substantive Rulemaking: Reconciling Principle and Expediency*, 125 U. PA. L. REV. 62, 77 (1976) ("[T]he state supreme courts have uniformly held that the legislatures are the only branch of government possessing the power to legislate.").

205. *See supra* Part I.B; *see also* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 587-88 (1957) ("In the framework of our Constitution, the President's power to see that the laws are faithfully executed refutes the idea that he is to be a lawmaker. The Constitution limits his functions in the lawmaking process to the recommending of laws he thinks wise and the vetoing of laws he thinks bad. And the Constitution is neither silent nor equivocal about who shall make laws which the President is to execute."); *id.* at 637-38 (Jackson, J., concurring) ("When the President acts in absence of either a congressional grant or denial of authority, he can only rely upon his own independent powers [granted by the Constitution] . . . . When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb . . . . Presidential claim to a power at once so conclusive and preclusive must be scrutinized with caution, for what is at stake is the equilibrium established by our constitutional system.").

206. Kyllo v. United States, 533 U.S. 27, 34 (2001).

frames the Fourth Amendment inquiry from whether the use of a particular technology is similar to the searches the Founders feared to whether the Founders would have enjoyed "that degree of privacy against government."[207] The *Kyllo* Court focused on the freedom from government surveillance enjoyed by the Founders rather than on the kinds of searches that concerned them. *Kyllo* limits the erosion of individual privacy and security brought on by new technologies by requiring the use of such technologies to be authorized by a warrant. More importantly, as discussed in Part IV, an approach based upon the Founders' privacy is a positive step toward returning to the people the authority to determine the extent and reasonableness of government's surveillance power.

Suspecting that Danny Kyllo was growing marijuana in his home, federal agents used a thermal imaging device, the Agema Thermovision 210, to scan Kyllo's home.[208] Growing marijuana indoors ordinarily requires the use of high-intensity lamps and, like all heat sources, these lamps emit infrared radiation. Thermal imagers are capable of detecting infrared radiation, which is imperceptible to the human eye, and "operates somewhat like a video camera showing heat images."[209] The scan of Kyllo's home revealed that the garage and a side of his home were relatively hotter than the rest of the home and substantially warmer than his neighbors' homes.[210] Based upon the scan and other information, a warrant was issued authorizing a physical search, which resulted in the discovery of more than one hundred marijuana plants.[211] The district court upheld the warrantless use of the device because in its estimation the device was relatively non-intrusive—it displayed only a crude visual image of heat, did not penetrate the walls or windows of the home, and did not reveal any intimate details.[212]

Writing for the majority, Justice Scalia begins by questioning the Court's assessment of "when a search is not a search."[213] Noting the disjuncture between the term "search" as it is commonly understood and as it is applied in Fourth Amendment law, Scalia recognized that the Court has applied

207. *Id.*
208. *Id.* at 29-30.
209. *Id.*
210. *Id.*
211. *Id.*
212. *Id.*
213. *Id.* at 31-32.

"somewhat in reverse the principle first enunciated in *Katz*" holding that "a Fourth Amendment search does *not* occur" unless the Court concludes that there is a reasonable expectation of privacy.[214] This odd state of affairs might be explained by the need to reconcile the common law principle that "'the eye cannot by the laws of England be guilty of a trespass'"[215] while preserving "somewhat" the doctrine that warrantless searches are presumptively unconstitutional.[216]

The opinion then abruptly shifts to the question confronting the Court, which according to the opinion is determining the limits, if any, upon the power of police technology to "shrink the realm of guaranteed privacy."[217] In defining these limits, Scalia describes the Court's role as assuring "preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[218] Consistent with this approach, the opinion holds at a minimum that searches of the interior of the home must be considered searches under the Constitution.[219] The Court noted, "We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use."[220] According to Scalia, this is a "ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*."[221] Any other conclusion "would . . . permit police technology to erode the privacy guaranteed by the Fourth Amendment."[222]

By focusing upon the Founders' privacy, Scalia's opinion casts aside means analysis. At first, this rejection is implicit as the majority reaches its conclusion without any examination of the factors discussed in Part II or relied upon by the lower courts. The rejection becomes explicit, however, in response to

---

214. *Id.*

215. Boyd v. United States, 116 U.S. 616, 628 (1886) (quoting Entick v. Carrington, 19 Howell's State Trials 1029 (K.B. 1765)).

216. *Kyllo*, 533 U.S. at 31-32.

217. *Id.* at 34.

218. *Id.*

219. *Id.*

220. *Id.* (citation omitted).

221. *Id.*

222. *Id.*

the argument of the Government and dissent that no search occurred because the device detected only heat radiating outside the house. That is, the police employed "off-the-wall" rather than "through-the-wall surveillance."[223] Justice Stevens's dissent is a perfect illustration of means analysis at work. According to Stevens, government use of the thermal imaging device in *Kyllo* should not be considered a search for several reasons.[224] First, the information was obtained from outside of the home without physically penetrating the premises.[225] Second, a person has no reasonable expectation of privacy in the heat emanating from the home because it is exposed to the public.[226] Third, the thermal imaging device did not reveal any intimate or embarrassing information about the home.[227] In rejecting these arguments, Scalia noted that the same analysis would permit warrantless searches with any device that simply records information emanating from the home including powerful microphones and satellites.[228] Moreover, Scalia criticized this type of reasoning as the same "mechanical interpretation of the Fourth Amendment" rejected in *Katz*—an approach that, like *Olmstead*, "leave[s] the homeowner at the mercy of advancing technology."[229] Consequently, Scalia concluded that the government must obtain a warrant before it may use these new technologies.[230]

As illustrated by the decision, preserving "the degree of privacy against government that existed when the Fourth Amendment was adopted" instead of determining whether a search is a search dramatically alters the protection afforded by the amendment. Rather than permitting government to expand its power to conduct surveillance because advances in technology distance information gathering from the physical searches of the eighteenth century, *Kyllo* limits government's ability to engage in warrantless searches to those considered reasonable at the time the amendment was adopted—most notably searches conducted by the unaided senses. The use of any technology to enhance those senses would require a war-

223. *Id.* at 35.
224. *Id.* at 41-44 (Stevens, J., dissenting).
225. *Id.*
226. *Id.*
227. *Id.* at 43-46 (Stevens, J., dissenting).
228. *Id.* at 35-37.
229. *Id.*
230. *Id.* at 40.

rant until that technology is in general public use.[231]

Consider once again the examples of the net-wide search/Magic Lantern, decryption, and Carnivore. As discussed in Part II, all three of these technologies might not have been considered searches under the means analysis. Under *Kyllo* there would be no question that government use of these technologies would represent searches. Because these technologies did not exist at the time the amendment was adopted and were therefore incapable of invading the Founders' privacy, in order to use them, law enforcement must first obtain a warrant. Instead of the hopelessly subjective analysis that typifies current Fourth Amendment analysis, the only questions remaining for the courts are objective: Did the police have a warrant or is the technology in general public use? For the purposes of this discussion, I will assume that *Kyllo*'s use of "general public use" means what it says: The technology must actually be routinely used by the general public and not simply available or used by some portion of the public.[232] My reasons for this assumption are discussed in Part IV. As the general public does not yet conduct net-wide searches, have the power to decrypt encrypted messages, or monitor and capture Internet information flow, a warrant would be required to authorize these searches.

Justice Scalia's opinion in *Kyllo* could be interpreted more narrowly as applying only to surveillance of the interior of the home. After all, the holding is specifically limited to the home,

---

231. *Kyllo's* approach is also preferable to the reasonable expectation of privacy analysis because it comes closer to applying the Fourth Amendment as written and provides a clear means of determining what the amendment requires. Some may criticize this approach as *Olmstead* in reverse, locking government into the surveillance technologies and techniques of the eighteenth century. If *Kyllo's* holding was based on the Fourteenth Amendment and substantive due process, this criticism might be valid as *Kyllo* would limit government's powers to those that existed at the time the amendment was adopted. The Fourth Amendment's limitations are different. Rather than absolutely denying government the power to conduct searches it limits the exercise of that power to circumstances in which government has probable cause. As such, the Fourth Amendment does not prohibit the government from benefiting from new technologies; it merely defines when those technologies may be used.

232. This would appear to be consistent with the majority's conclusion that the thermal imaging device in *Kyllo* was not in general public use. 533 U.S. at 34. This, despite the fact that, as the dissent points out, there are thousands of Thermovision 210s or similar devices that were manufactured and "readily available to the public" for purchase or rent. *Id.* at 47 n.5 (Stevens, J., dissenting) (citing App. at 18); *see also id.* at 50 n.6 (noting that thermal imaging is not "routine").

a "constitutionally protected area," and the security of the interior of the home figures prominently throughout the Court's discussion and throughout this nation's history.[233] Limiting *Kyllo* to the interior of the home, however, would run counter to the Court's return to the true meaning of *Katz* and the rejection of mechanical interpretations of the Fourth Amendment. Such a narrow interpretation would instead return Fourth Amendment analysis to *Olmstead* and not *Katz*, a result the majority clearly wanted to avoid. Moreover, limiting *Kyllo* to the interior of the home does nothing to limit government power and discretion outside of the home. While *Kyllo* clearly has the potential to alter the Court's current interpretation of the Fourth Amendment, should it be embraced? Part IV argues that courts should apply the *Kyllo* analysis not because it is better at protecting privacy or protects more privacy, but because it preserves the right of the people to determine what powers the government should have to engage in surveillance and when that power should be considered reasonable.[234]

IV. THE PEOPLE'S POWER

Prior to *Kyllo*, the Supreme Court's jurisprudence had transformed the Fourth Amendment from a provision circumscribing government power and discretion to one accommodating such power and discretion; only the sophistication of its technology limited the government's power.[235] This transformation occurred because the Court limited the Fourth Amendment's protection to privacy and then narrowly interpreted privacy to create exceptions to the types of searches governed by the amendment. Through this doctrine, the Court presumed that the government could employ new surveillance technologies unless the surveillance invaded interests the Justices subjectively considered private. The people's only role in the process was to respond to government and the courts after the fact. They were relegated to enacting legislation to limit government

233. *Id.* at 34 (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

234. As Justice Stevens notes, *Kyllo* can be interpreted as under-protective of privacy because of the general public use exception. *Id.* at 46-48 (Stevens, J., dissenting). In this respect, as evidenced by the general public use exception, Justice Scalia's continued reliance upon privacy suffers from some of the same flaws as the rest of the Court's Fourth Amendment jurisprudence. The definition of general public use will be discussed in greater detail in Part IV.A.

235. *See supra* Part II.

use of technology or amending the Constitution.[236] This section outlines why the Supreme Court's decision in *Kyllo* creates an opportunity to return the people to their rightful position as the primary source and arbiter of governmental power. Depending upon how the Court determines what makes a search reasonable under the amendment, the Supreme Court may reinforce self-governance in two ways. If the Court maintains the per se rule against warrantless searches, which I will describe as the "moderate thesis," popular sovereignty is reinforced through the Fourth Amendment's Warrant Clause. As Part IV.A argues, this result is a perfectly reasonable and acceptable interpretation of the amendment, and consistent with the principles of constitutional self-governance. If the Court chooses to expand its interpretation of reasonableness, the "radical thesis," Part IV.B argues that reasonableness should only be expanded to include surveillance technologies authorized and circumscribed by statute subject to judicial review. Under both of these approaches, the people, as the Founders intended, would determine the reasonableness of government power.

A. "WARRANTLESS SEARCHES ARE UNLAWFUL"—THE MODERATE THESIS

Relying upon *Kyllo*, the Fourth Amendment may be interpreted to prohibit any government use of surveillance technology not in general public use unless authorized by a warrant. While this interpretation of the amendment may assign more weight to the Warrant Clause than some believe the Founders might have intended,[237] it nonetheless remains true to the Fourth Amendment's ultimate purpose of protecting the people's right to determine the reasonableness of searches. A per se rule simply shifts the vehicle for this determination from the common law jury to the Constitution itself.

As the discussion of the amendment's pre-constitutional origins demonstrates, the Fourth Amendment could recognize two methods for determining when searches are reasonable.[238] Government could conduct a search without a warrant provided that the people had the power to oversee those searches directly. Otherwise, government must obtain a warrant sup-

236. Of course, the people may even indirectly influence this process by electing executives who promise to alter governmental practice and/or nominate judges whose views on privacy are more consistent with their own.

237. *See supra* Part I.

238. *See supra* Part I.

ported by probable cause. Even though the Founders might have been concerned about warrants, the Fourth Amendment considers warrants reasonable when they are supported by "probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[239] While a per se warrant rule eliminates one method for determining reasonableness, a rigid adherence to the Warrant Clause still applies the people's definition of reasonableness as expressed in the clause. Accordingly, a per se rule remains faithful to the amendment's purpose of ensuring that the people determine when government may search. As discussed in Part II, the problem with pre-*Kyllo* search and seizure cases was not the per se warrant rule, but rather the Court's willingness to create exceptions to the rule. By creating exceptions to the per se rule, the Justices replaced the judgment of the people with their own.

Given the importance of strictly adhering to the warrant requirement under a per se rule, *Kyllo*'s exception for technologies in general public use would appear inconsistent with the right of the people. Granted, a general public-use exception would be based upon the same underlying flaw as the Court's earlier Fourth Amendment jurisprudence, that the amendment protects privacy and not power, and whether members of the public may invade our privacy does not answer the question of whether government may. Similarly, if the Court were to interpret this exception broadly, general public use could become an exception that swallows the rule much like *Katz*'s statement regarding what one voluntarily exposes to the public. Moreover, as Justice Stevens argued, creating an exception for technologies in general public use seems "perverse because it seems likely that the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available."[240] Perhaps, in light of these concerns, Scalia's opinion appears to suggest that the Court may be open to reexamining the factor.[241]

Despite these concerns, the exception might be acceptable precisely because it is based upon an increased threat to privacy. If limited to only those technologies already routinely used by the general public, the exception would apply only un-

239. U.S. CONST. amend. IV.
240. Kyllo v. United States, 533 U.S. 27, 47 (2001) (Stevens, J., dissenting).
241. *Id.* at 50 n.6.

der circumstances in which the public as a whole understands the risks and has borne the costs of such technologies. A strict interpretation of general public use, therefore, reduces the risk that the public will acquiesce to government use of technology because a majority or powerful minority have not internalized the costs of such technology, and therefore either misperceive the relative costs and benefits or selfishly are willing to allow others to pay them.[242] If society is to rely upon legislatures to protect against governmental invasions of privacy or security, it is only appropriate to do so when the use of a technology is so ubiquitous that the public as a whole appreciates its threat. Only then can we be assured that the absence of legislative safeguards results from the public's judgment that the threat is acceptable rather than its lack of concern for or discrimination against a subset of the population.

While a per se warrant requirement might be doctrinally neater without any exceptions, the general public use exception may very well be consistent with the common law origins of the amendment and avoids its own unduly mechanical interpretation of the amendment.[243] As Justice Scalia recognized in *Kyllo*, one of the problems with interpreting the Fourth Amendment's prohibition against warrantless searches was the common law conclusion that the eyes cannot be guilty of trespass.[244] If the police could use their eyes and ears to gather information without a warrant, then the Fourth Amendment implicitly recognized at least some exceptions from the beginning. What is important about the common law rule for natural senses is not its pedigree or its historical existence, but rather the reason for the exception. Natural senses are by default surveillance tools routinely used by the general public. The public, therefore, has always understood the threat to privacy and security represented by these senses and has responded

242. Wasserstrom & Seidman, *supra* note 25, at 95 (noting that as "the cost of law enforcement is more widely distributed, . . . there is less reason to fear that the governmental decisions to trade off privacy for law enforcement are being made without considering everyone's interests equally").

243. This does not address the question of whether a warrant should, nonetheless, be required because of concerns over police discretion with respect to micro-level decisions (i.e., decisions regarding when technologies should be used to search a particular suspect). Others have identified some of the concerns the public use exception creates at that level. *See* Slobogin, *supra* note 26.

244. *Kyllo*, 533 U.S. at 31-32 (citing Boyd v. United States, 116 U.S. 616, 628 (1886)).

accordingly by building walls and fences and prohibiting physical trespass. Technology should be no different. To the extent that flashlights, cameras, and binoculars are routinely in general public use, we become as familiar with the threats they pose as we have with unaided sight. Likewise, we become as capable of evaluating and responding to the technology's threat either with privacy enhancing technology or by limiting its use by law. While it might be reasonable to require the government to obtain a warrant even for such technologies, interpreting the Fourth Amendment to require one because of macro-level decisions could be considered unduly formalistic.

One serious objection to the general public use exception is that formalism serves an important value in this context because government use of technology is different. To the extent that the Fourth Amendment is truly about power rather than privacy, the fact that citizens may invade each other's privacy does little to answer the question of whether government should have the same power.[245] No longer slavishly focusing on privacy, a per se warrant requirement should arguably apply to any new technologies. While one might respond that in light of the pervasiveness of the technology, the political process can be trusted to do what the people think necessary, or that even the doctrine of separation of powers recognizes that some executive powers may be authorized through legislative acquiescence,[246] the objection nonetheless deserves serious attention.

On the other side, one might note that requiring probable cause before law enforcement may employ an arguably less intrusive technological search may create a disincentive for using those technologies. After all, why would the police use a crude thermal imaging device if they have sufficient justification for conducting a physical search even though the thermal imaging device may be less intrusive and a more efficient means of excluding the innocent? In some instances, law enforcement may choose to conduct a physical search rather than resorting to technology; it is far from clear, however, that they will automatically prefer physical searches to technological searches. On balance, technological surveillance may often be superior to

245. *See* Amsterdam, *supra* note 9, at 406-07.

246. *See* Dames & Moore v. Regan, 453 U.S. 654, 688 (1981) (concluding that Congress had implicitly authorized the practice of claim settlement by executive agreement); Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 610-11 (1952) (Frankfurter, J., concurring) (recognizing that under some circumstances Congress may implicitly authorize executive actions).

physical searches precisely because certain technologies may make it possible to exclude suspects with less effort and intrusion than a physical search. Likewise, technological searches may be superior to physical searches because they permit law enforcement to gather information without alerting suspects to the investigation. These searches reduce the risk that evidence will be destroyed, lead to additional evidence of criminal conduct, and help identify additional suspects. Most importantly, technologically assisted surveillance may allow law enforcement to gather information from a safe distance without having to expose agents to physical harm. Lastly, to the extent that this is a subject for debate and discussion, it is either an argument against recognizing a per se rule under the Fourth Amendment, or an argument for amending the Constitution.

From a policy perspective, supporters of effective law enforcement should favor this moderate thesis. First, under the Fourth Amendment, law enforcement could adopt technology without the need for legislative authorization. While this type of executive action may still be suspect under general separation of powers principles, the Fourth Amendment would not prohibit it because the warrant requirement guarantees that the people have determined the reasonableness of the search.[247] Second, obtaining a warrant is not a significant burden on law enforcement,[248] and it brings with it a tremendous benefit—insulating the search from subsequent constitutional challenge.[249] *Kyllo* could become the Fourth Amendment equiva-

247. As noted at the beginning of this Article, I am assuming for purposes of this discussion that the existence of Fourth Amendment restrictions upon government's power to adopt surveillance technologies and to conduct searches would satisfy separation of powers concerns. An argument could be made, however, that reasonableness can be read as imposing obligations in addition to those embodied in the Warrant Clause, including that a search is not reasonable even if supported by a warrant if the search was not authorized by statute.

248. Of course, one may argue that if law enforcement must have probable cause to use arguably less intrusive technologies, they would have no reason to do so because they would have sufficient justifications for conducting a physical search. It may be true in some instances that law enforcement may simply choose to conduct a physical search rather than use a thermal imaging device, Carnivore, or a tracking device. Law enforcement may, however, choose technological surveillance over physical surveillance because of the various benefits derived from technological searches, including reduction in physical risk to law enforcement and the ability to gather information without alerting the suspect to the investigation.

249. *See, e.g.*, Donald L. Beci, *Fidelity to the Warrant Clause: Using Magistrates, Incentives, and Telecommunications Technology to Reinvigorate Fourth*

lent of *Miranda* warnings[250] with the warrant requirement serving as a prophylactic rule benefiting government actors more than it limits their behavior.[251] Third, *Kyllo* provides clear guidance to law enforcement on the use of surveillance technologies, and virtually eliminates the uncertainty associated with the use of new technologies. The only uncertainty will be at the margins when it comes to determining whether the general public routinely uses a particular technology. Fourth, applying the warrant requirement equally to all technologies (and arguably all search techniques) limits the potential for judicially created exceptions to encourage differential enforcement of criminal laws.[252] Lastly, in contrast to the radical thesis, the moderate thesis requires no changes in constitutional law outside the Fourth Amendment.

B. "NOT ALL WARRANTLESS SEARCHES ARE UNLAWFUL"—THE RADICAL THESIS

For decades, commentators have criticized the Supreme Court for limiting the Fourth Amendment's definition of reasonableness to warrants.[253] In particular these commentators have argued that expanding Fourth Amendment reasonableness to include searches authorized and circumscribed by statute or administrative rulemaking would better serve the amendment's goal of limiting police discretion while promoting responsible police behavior and accountability in ways that the Court's all or nothing approach cannot.[254] In certain areas of Fourth Amendment law, the Court has in fact relaxed the warrant requirement in reliance upon statutory authorization or

---

Amendment Jurisprudence, 73 DENV. U. L. REV. 293, 317 (1996) ("As a second incentive for government agents to use warrants, the burden of production and persuasion should be placed on the defendant if a warrant has been obtained to show that a search or seizure is unconstitutional.").

250. Miranda v. Arizona, 384 U.S. 436 (1966).

251. Stephen J. Schulhofer, Miranda's *Practical Effect: Substantial Benefits and Vanishingly Small Social Costs*, 90 NW. U. L. REV. 500, 554 (1996). *But see* Paul G. Cassell, Miranda's *Social Costs: An Empirical Reassessment*, 90 NW. U. L. REV. 387, 389-91 (1996).

252. *See* Stuntz, *supra* note 6, at 1047.

253. *See* AMAR, *supra* note 29, at 68-69; Amsterdam, *supra* note 9, at 358-59, 367-68; Wayne R. LaFave, *Controlling Discretion by Administrative Regulations: The Use, Misuse, and Nonuse of Police Rules and Policies in Fourth Amendment Adjudication*, 89 MICH. L. REV. 442, 449-50, 468-70 (1990).

254. *See, e.g.*, Amsterdam, *supra* note 9, at 423-28; LaFave, *supra* note 253, at 451.

administrative rules to uphold warrantless searches.[255] *Kyllo's* conclusion that the use of surveillance technologies not routinely used by the general public is a search will most likely prompt others to argue that the Court should expand its definition of reasonableness to include warrantless searches pursuant to statute and administrative rules. As Part IV.A suggests, this expansion is not required or even desirable, but if it should occur, government use of technology absent a warrant should only be considered reasonable when authorized by statute subject to judicial review. Only under these circumstances would the Fourth Amendment guarantee that the people determine the reasonableness of government searches, and follow the Constitution's separation of powers.[256]

While having law enforcement develop and implement a process for administrative rulemaking is certainly valuable and worthwhile regardless of its Fourth Amendment implications, it should not be allowed to replace warrants under the amendment. As discussed earlier, police decisionmaking and discretion can be separated into micro level decisions and macro level decisions.[257] Requiring the police to formulate internal rules and policies governing searches is a significant step towards limiting police discretion at the micro level, that is, when and how to conduct searches. Administrative rulemaking, however, does nothing to alleviate executive discretion at the macro level whether law enforcement should have the power to conduct

---

255. *See, e.g.*, Griffin v. Wisconsin, 483 U.S. 868, 872-73 (1987) (upholding state regulations authorizing probation officers to conduct warrantless searches of probationer homes based upon "reasonable grounds"); New York v. Burger, 482 U.S. 691, 711 (1987) (upholding warrantless inspection of an automobile scrap yard because a "statute informs the operator of a vehicle dismantling business that inspections will be made on a regular basis"); Donovan v. Dewey, 452 U.S. 594, 603 (1981) (upholding warrantless inspection of coal mines under the Federal Mine Safety and Health Act provided that the inspection program "provide[] a constitutionally adequate substitute for a warrant[]");Colorado v. Bertine, 479 U.S. 367, 374 (1987) ("[R]easonable police regulations relating to inventory procedures administered in good faith satisfy the Fourth Amendment, even though courts might as a matter of hindsight be able to devise equally reasonable rules requiring a different procedure."). This limited relaxation of the warrant requirement in areas outside of day-to-day criminal investigation has been criticized as a form of privacy *Lochner*ism. *See* Stuntz, *supra* note 29, at 442; Stuntz, *supra* note 6, at 1047.

256. Of course, one could also expand reasonableness to once again recognize the role of the common law jury. *See* AMAR, *supra* note 29, at 70. Doing so, however, would require the Supreme Court to re-examine its positions on sovereign immunity, official immunity, and habeas corpus.

257. *See supra* Part II.

such searches at all. Allowing administrative rulemaking to replace the warrant requirement would suffer from the same fundamental problem of unbounded executive discretion pre-*Kyllo*. A dialogue on reasonableness would simply replace the dialogue on privacy with law enforcement and the judiciary calling the shots.

In contrast, requiring the use of surveillance technologies to be authorized by statute recognizes that the people should determine just how much power government should wield. As discussed earlier, popular control over government's power to search was the driving force behind the adoption of the Fourth Amendment. Moreover, requiring statutory authorization for law enforcement's power to search—even if it is not used to determine reasonableness—would bring search and seizure law in line with the doctrine of separation of powers governing executive power in general. Outside the Fourth Amendment, the Supreme Court is highly skeptical of the executive branch defining its own powers.[258] Allowing law enforcement to determine what powers it may exercise in the absence of constitutional or legislative authorization effectively grants the officer on the street or the chief of police greater power than the Chief Executive.

In addition to being the proper constitutional body to decide these questions, legislatures are institutionally more competent than courts to make the types of policy decisions associated with authorizing government surveillance. Because they are politically accountable, they are more likely to evaluate the policy implications of certain surveillance technologies, balancing, among other things, the threat to privacy and potential for abuse against the needs of law enforcement and the interests of public safety considering the interest of the public in general. They are also better able to develop a factual record with respect to the nuances and details of new technologies and their costs and benefits. Moreover, whatever one might think of the legislative process, it is more likely to take the interests of the general public into account in fashioning rules governing surveillance than courts who are asked to make such decisions in cases in which a search revealed evidence of a defendant's guilt and the only remedy is exclusion of that evidence.

Of course, allowing legislatures to determine government's

258. *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 587-88 (1952).

power to search raises concerns about abuse or unresponsive legislative power. Admittedly, strict adherence to the warrant requirement avoids this problem by denying legislatures any power to deviate from the Warrant Clause.[259] Concerns about legislative abuse, however, should be alleviated by judicial review of these legislative determinations with the Warrant Clause as the guide. As the Supreme Court has done in the context of administrative searches, it should review statutory grants of power to determine whether the procedures adopted by legislatures are "constitutionally adequate substitute[s] for a warrant."[260] Using the Warrant Clause as the touchstone for evaluating statutory safeguards would limit deviations from the amendment's stated safeguards while ensuring that the legislation limited arbitrary and abusive searches.[261] Judicial review under these circumstances would return the judiciary to its traditional constitutional role of evaluating such judgments against a backdrop of constitutional principles and norms rather than allowing judges to sit as policymakers themselves. Ultimately, however, the majoritarian concern goes directly to the larger question of whether reasonableness under the Fourth Amendment should be expanded beyond the warrant requirement at all.

Could Congress or a state legislature satisfy the Fourth Amendment requirement of reasonableness by simply passing a law authorizing law enforcement to adopt and use any technology it chooses? Assuming that a legislature would pass such a statute, a highly dubious proposition, the answer must be no. While such a statute might satisfy the doctrine of separation of powers, it does nothing to address the concerns embodied in the

---

259. Of course, one may argue that the tyranny of contemporary majorities is simply replaced by the tyranny of past majorities.

260. *Donovan*, 452 U.S. at 603.

261. Of course, the legislation should be subject to review in light of other constitutional concerns including equal protection. As one author has noted,

> The warrant requirement injects the judgment of a "neutral and detached" magistrate and also has what may be the more important effect of compelling a contemporaneous recordation of the factors on whose basis the action is being taken. The probable cause requirement obviously can't guarantee a lack of arbitrariness: invidious choices among those respecting whom there is probable cause are possible. By setting a substantive parameter at one end of the decision, however, it at least requires that persons not be singled out for arrest or search in the absence of strong indication of guilt, that is, on the basis of constitutionally irrelevant factors alone.

ELY, *supra* note 19, at 172-73.

Fourth Amendment. Such a statute does nothing to limit police discretion at either the macro or micro level.[262] While legislatures may delegate broad discretionary powers to the executive branch in other areas of constitutional law, the Fourth Amendment would appear to limit such a delegation with respect to searches and seizures.

CONCLUSION

The debate over the proper scope of the Fourth Amendment in general, and its relationship with information gathering technologies in particular, constitutes a debate over the proper distribution of power in our constitutional government. Who determines what technologies may be used to gather information about individuals and the public in general? In other words, who determines just how much security the people may enjoy? For more than a quarter of a century this decision was made occasionally by judges, but more often by law enforcement engaged in the surveillance. Not only has this permitted technology to erode individual privacy, but it is contrary to the central purpose of the Fourth Amendment. In adopting the amendment, the Framers of our Constitution were primarily concerned with limiting government power and discretion, and like all governmental power, the decision of how much surveillance power the government should have was left to the people. In debating over how to define privacy, the courts have ignored these concerns for far too long.

This Article has argued that the Fourth Amendment cannot be viewed in isolation, but must be seen as a complement to other constitutional protections including the doctrine of separation of powers. The Fourth Amendment and the definition of executive power in our constitutional separation of powers protect the public from arbitrary and unrestrained executive power. The need for this interpretation becomes clear when we recognize that certain decisions made by law enforcement are more than simply discretionary decisions about when to search a particular individual, but rather macro level decisions that determine the extent of their own powers and correspondingly the amount of privacy the public may enjoy. Accordingly, I

262. This conclusion would also appear consistent with the colonial response to the writs of assistance, which were condemned even though they were authorized by acts of parliament. *See supra* Part I.A. *See generally* SMITH, *supra* note 34 (discussing the colonial controversy surrounding the writs of assistance).

have argued that the Fourth Amendment requires that searches conducted with new surveillance technologies must be treated as searches subject to Fourth Amendment restraints. Technologically assisted searches must either comply with the Warrant Clause or be authorized by a statute containing safeguards that are constitutionally adequate substitutes for a warrant. While this Article has focused on law enforcement decisions to adopt new surveillance technologies, the concerns it raises about existing Fourth Amendment law are not limited to technology. Law enforcement decisions to use undercover agents, helicopters, or automatic weapons in combating crime are all decisions that determine the scope of executive power and the level of privacy and security the public may enjoy. To the extent that the Supreme Court interprets the Fourth Amendment in such a way that it no longer serves as a check against arbitrary government decisionmaking in these areas as well, the constitutional questions are equally troubling. It may be expedient or more efficient to leave certain decisions to the executive branch rather than subject them to the limits imposed by the Constitution or to require legislative authorization and safeguarding, especially in times of crises. Our Constitution, however, was not adopted to promote efficiency but to preserve liberty, and there is no more important means of preserving individual liberty than prohibiting the exercise of arbitrary power. While these institutions and principles may be destined to pass away, "it is the duty of the Court to be [the] last, not [the] first to give them up."[263]

263. *Youngstown Sheet & Tube*, 343 U.S. at 655 (Jackson, J., concurring).