IS THE COURT ALLERGIC TO *KATZ*? PROBLEMS POSED BY NEW METHODS OF ELECTRONIC SURVEILLANCE TO THE "REASONABLE-EXPECTATION-OF-PRIVACY" TEST

COLIN SHAFF*

"The courts are better suited to resolve the complex and case-specific issues relating to constitutional search-and-seizures protections."

California Governor Edmund Gerald "Jerry" Brown[1]

"The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."

City of Ontario v. Quon[2]

"Applying the Fourth Amendment to new technologies may sometimes be difficult, but when it is necessary to decide a case we have no choice."

City of Ontario v. Quon, (Scalia, J., concurring).[3]

* Juris Doctor Candidate 2014, University of Southern California Gould School of Law. The author would like to thank Julianna Lassleben for her encouragement, support, and tolerance during my law school career, and especially during the writing of this Note. The author would also like to thank the editorial staff of the *Southern California Interdisciplinary Law Journal* for its efforts.

1. Hanni Fakhoury, *Governor Brown Vetoes Warrant Protection for Cell Phones* (Oct. 11, 2011), https://www.eff.org/deeplinks/2011/10/governor-brown-vetoes-warrant-protection-cell-phones (quoting Governor Brown's veto statement of California legislation (SB 914) that would have required law enforcement to obtain a warrant before searching information on a cell phone).

2. City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010).

3. *Id*. at 2635 (Scalia, J., concurring).

I. INTRODUCTION

The Fourth Amendment provides a bulwark against government intrusion by barring "unreasonable searches and seizures."[4] However, the U.S. Supreme Court has faced considerable difficulty in determining what government actions are "unreasonable" and what actions constitute a "search" or "seizure." These long-standing difficulties have led legal scholars to condemn the Court's Fourth Amendment jurisprudence as "famously zigzagging,"[5] providing a "byzantine patchwork of protections,"[6] and creating "a contentious jurisprudence that is riddled with inconsistency and incoherence."[7] In sum, "most commentators have recognized that . . . Fourth Amendment doctrine is in a state of theoretical chaos."[8] This is especially true regarding the Court's approach to electronic surveillance.

Moreover, federal legislation concerning electronic surveillance is not any more consistent or comprehensive. When Congress has acted to address the privacy implications of technological developments, it "has created an uneven fabric of protections that is riddled with holes and that has weak protection in numerous places."[9] In addition, because Congress acts so slowly, federal statutes do not regulate many now-commonplace technologies like the Global Positioning System ("GPS") surveillance are not regulated by federal statute.[10] As such, technological development has outpaced both legislative regulation and judicial review.[11]

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

5. David A. Sklansky, *Back to the Future: Kyllo, Katz, and Common Law*, 72 MISS. L.J. 143, 143 (2002).

6. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 479 (2011).

7. Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1511 (2010).

8. *Id.* at 1512 (quoting Donald R.C. Pongrace, *Stereotypification of the Fourth Amendment's Public/Private Distinction: An Opportunity for Clarity*, 34 AM. U. L. REV. 1191, 1208 (1985)).

9. Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 766 (2005).

10. *Geolocation Privacy Legislation*, GPS.GOV, http://www.gps.gov/policy/legislation/gps-act (last updated Apr. 10, 2013). Three bills addressing GPS and geolocation privacy were introduced between 2011 and 2013, but none were considered for a vote.

11. Solove, *Fourth Amendment Codification*, *supra* note 9, at 769 ("Congress, however, has not done a good job [of creating new rules] and its rules regulating electronic surveillance are hopelessly out of date.").

The mutual failure of Congress and the Court to respond adequately to the privacy implications of technological change was publically demonstrated on November 9, 2012, when Central Intelligence Agency ("CIA") director David Petreaus resigned his position following an investigation by the Federal Bureau of Investigation ("FBI").[12]

The investigation that resulted in his resignation began in May 2012, when a woman in Florida received a number of anonymous, harassing emails, some of which included details about certain high-ranking military officers stationed in Florida.[13] Although the FBI rarely, if ever, investigates this kind of online harassment, it chose to investigate this case in part because the emails referred to military personnel and also because the woman had a personal relationship with an FBI agent.[14]

The FBI began its investigation by determining the geographical origin of the messages.[15] The location information contained in emails, as well as other information like the email address of the sender and recipient, are regulated by Title III (the Pen-Register Act) of the Electronic Communications Privacy Act ("ECPA").[16] This statute allows the government to access certain information contained in emails by simply certifying that "information likely to be obtained . . . is relevant to an ongoing investigation" and does not require showing probable cause for the search.[17]

Having analyzed the location information of the threatening emails, the FBI determined that they had been sent from hotels in various cities and also discovered that Paula Broadwell, Petreaus's biographer, had been present at the various locations when the emails were sent.[18] Based in part

12. Julian Sanchez, *Collateral Damage of Our Surveillance State*, REUTERS.COM (Nov. 15, 2012), http://blogs.reuters.com/great-debate/2012/11/15/collatoral-damage-of-our-surveillance-state.

13. *Id.*

14. *Id.*

15. Kim Zetter, *Email Location Data Led FBI to Uncover Top Spy's Affair*, WIRED.COM (Nov. 12, 2012, 2:17 PM), http://www.wired.com/threatlevel/2012/11/gmail-location-data-petraeus. All email messages contain a "header" that includes certain information, including information about the route through which the message traveled before reaching the recipient. The FBI was able to use this information to determine where the messages originated. *Id*.

16. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 (2013).

17. Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1287–88 (2004).

18. It is unclear exactly how the FBI matched the geographical information in the emails to the physical movements of Ms. Broadwell. *See* Evan Perez, Siobhan Gorman & Devlin Barrett, *FBI Scrutinized on Petraeus: Complaints by Female Social Planner Led to Email Trail That Undid CIA*

on the email location information, the FBI obtained a warrant to monitor all of Broadwell's email accounts.[19] Emails stored on a server are governed by Title II (the Stored Communications Act) of the ECPA.[20] Title II requires a warrant based on probable cause to search emails less than 180 days old; however, for emails older than 180 days, only a subpoena is required, and a supervisory official may issue the subpoena upon a showing of "specific and articulable facts showing . . . reasonable grounds [that the] communications are relevant to the criminal investigation."[21]

Moreover, because the FBI investigation involved national security, it may have been governed by the Foreign Intelligence Surveillance Act[22] ("FISA"), instead of the EPCA. FISA provides the government broad powers of investigation so long as foreign intelligence gathering is "a significant purpose" of the investigation.[23] FISA surveillance can be carried out pursuant to a court order granted by a secret panel of eleven district court judges.[24] While the government is required to obtain a warrant when the target of FISA surveillance is within the United States or is a U.S. citizen, the government may monitor the communications of U.S. citizens without a warrant when they are not the direct target of the surveillance.[25]

The FBI initially examined Broadwell's emails to determine if she posed a threat to national security, but instead discovered that she had been having an affair with Petreaus.[26] Although the FBI investigation did not reveal any evidence of a crime and did not lead to any criminal charges, the investigation resulted in the government obtaining very intimate

Chief, WALL ST. J. (Nov. 12, 2012, 9:57AM), http://online.wsj.com/news/articles/SB10001424127887324073504578113460852395852.

19. Zetter, *supra* note 15.

20. Stored Communications Act, 18 U.S.C. §§ 2701–2711 (1986).

21. Solove, *Reconstructing Electronic Surveillance Law*, *supra* note 17, at 1284. The definitions of "stored communications" and the scope of the legislation is vastly complicated; in general, all electronic communications, except unopened emails newer than 180 days, may be accessed with a subpoena, which may be issued by a supervisory official upon a showing of relevance, and in the case of administrative subpoenas, without judicial oversight. Notice of the search may not be required if the official certifies that notice would "jeopardize a pending investigation." Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1570 (2004).

22. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 (2013).

23. Solove, *Reconstructing Electronic Surveillance Law*, *supra* note 17, at 1290–91.

24. *Id.* at 1289.

25. STEPHEN J. SCHULHOFER, MORE ESSENTIAL THAN EVER: THE FOURTH AMENDMENT IN THE TWENTY-FIRST CENTURY 158–59 (2012).

26. Zetter, *supra* note 15.

information which, when it became public, led directly to Petreaus's resignation as director of the CIA.[27] Because the FBI was required to obtain a warrant only to search Broadwell's most recent emails, much of the investigation was pursued without having to demonstrate probable cause for the surveillance. The gaps in the statutory and constitutional protections of electronic communications gave great latitude to the FBI investigators, and Broadwell and Petreaus suffered the consequences.

This Note will examine the way in which the Court and Congress have reacted to the challenges posed by emerging technology with regards to the Fourth Amendment's "unreasonable search and seizure" clause. This Note argues that the best balance between protecting personal liberties and respecting the needs of law enforcement occurs when the Court, Congress, and state legislatures collaborate to craft robust statutory schema; in contrast, when the Court makes decisions without legislative input or when Congress acts without judicial guidance, the resulting law is often inadequate or incomplete. Section II will discuss the development of the Wiretap Act as an example of collaboration between state legislatures, the Supreme Court, and Congress, which resulted in a lasting, robust, and coherent statutory framework for telephone surveillance. Section III will closely examine two of the Supreme Court's recent cases concerning technology and the Fourth Amendment, *Kyllo v. United States*[28] and *United States v. Jones*,[29] and will demonstrate the Court's difficulties with integrating newly developed electronic surveillance techniques into its Fourth Amendment jurisprudence. In Section IV, this Note will suggest that state legislatures may play a key role in developing Fourth Amendment jurisprudence by being an important evidentiary resource to help the Court determine the "subjective expectation[s] of privacy . . . that society is prepared to recognize as 'reasonable.'"[30] This Note concludes by suggesting that the Court should reconsider its modern approach to the Fourth Amendment, and that state and federal legislatures should be encouraged to regulate government use of emerging electronic surveillance technologies.

27. Alanne Orjoux et al., *Timeline of the Petreaus Affair*, CNN.COM (Nov. 15, 2012, 12:01 PM), http://www.cnn.com/2012/11/12/politics/petraeus-timeline/index.html.

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

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

30. Katz v. United States, 389 U.S. 347 (1967) (Harlan, J., concurring).

II. BOOTLEGGERS AND GAMBLERS: WIRETAPPING, THE FOURTH AMENDMENT, AND THE ROLE OF THE STATES

In the eighteenth and early nineteenth centuries, the Fourth Amendment played a minor role in search and seizure cases.[31] Most search and seizure rules were based on state statutes and interpreted by state courts.[32] Moreover, although a number of states had constitutional provisions that mirrored the language of the Fourth Amendment, the state interpretation of those provisions often differed from the Supreme Court's interpretation of the Fourth Amendment.[33] Indeed, federal search and seizure jurisprudence was negligible until 1919, when the National Prohibition Act[34] led to a dramatic increase in the number of federal prosecutions, and the resulting use of wiretaps by federal investigators led to evidentiary and constitutional challenges to federal searches.[35]

The importance of state-based search and seizure legislation is especially clear in wiretap law. Long before the federal government first regulated wiretapping in the Federal Communications Act of 1934,[36] the states were concerned by the expansion of telephone and telegraph communications and enacted statutes prohibiting wiretapping by private parties.[37] In contrast, wiretapping remained largely unregulated by federal

31. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 842 (2004) (stating that "[t]he Supreme Court mentioned the Fourth Amendment in only about two dozen cases in the first 130 years of the Amendment's existence, and actually interpreted the Amendment only a handful of times during that period" and moreover, of the few search and seizure cases that came before the Court, Fourth Amendment protections were rarely extended beyond the enumerated categories of "persons, houses, papers and effects").

32. David E. Steinberg, *The Uses and Misuses of Fourth Amendment History*, 10 U. PA. J. CONST. L. 581, 587 (2008).

33. Stephen Kanter, *Sleeping Beauty Wide Awake: State Constitutions As Important Independent Sources of Individual Rights*, 15 LEWIS & CLARK L. REV. 799, 801 (2011) ("[S]tate constitutionalism was a central part of the original plan of the eighteenth-century United States Constitution and Bill of Rights . . . [and because] a number of the original states already had state constitutional bill-of-rights provisions before the United States Constitution was written . . . people expected the states to secure and protect the rights of their own individual citizens."). *See generally*, Michael J. Gorman, *Survey: State Search and Seizure Analogs*, 77 MISS. L.J. 417 (2007) (surveying state legislation of search and seizure, and noting the variations from federal legislation or constitutional precedent).

34. National Prohibition Act, ch. 85, 41 Stat. 305 (1919) (repealed 1935).

35. Kerr, *supra* note 31, at 842–43 ("[N]o published federal cases mentioned wiretapping before the Prohibition era.").

36. Communications Act of 1934, ch. 652, 48 Stat. 1064 (current version at 47 U.S.C. § 605 (2000)).

37. ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 157–58 (2004). An emergency federal ban on wiretapping was

law and more or less widespread, despite many members of the federal government regarding wiretapping as unethical.[38]

A. OLMSTEAD V. UNITED STATES[39]

After the passage of the National Prohibition Act and the consequent rise of bootlegging, the number of federal prosecutions expanded exponentially; at the same time, the increasing ubiquity of telephone communications made wiretaps an important law enforcement tool.[40] Although the U.S. Attorney General officially repudiated use of wiretaps, and both the Treasury Department and the FBI supported a ban on wiretapping, this prohibition was not consistently followed.[41]

In the early 1920s, a government agent defied Washington state law and the policy of the Department of Justice by using a warrantless wiretap to discover the details of James Olmstead's smuggling operation.[42] Despite the government making only a "half-hearted defense of the wiretapping investigation" in *Olmstead*,[43] the Supreme Court found that the wiretap was not a Fourth Amendment search so long as the government did not physically penetrate the "houses or offices of the defendants" in placing the wiretap.[44] The Court did not find the state prohibition of wiretapping to be

enacted in 1918, in conjunction with the government seizure of telephone and telegraph lines during World War I. However, that ban expired a year later and was not renewed. Kerr, *supra* note 31, at 841. *See also* Donnelly, *infra* note 38, at 779.

38. Richard G. Donnelly, *Comments and Caveats on the Wire Tapping Controversy*, 63 YALE L.J. 799, 779–80 (1954) ("[W]ire tapping was a common practice both in and out of government until 1924 when Attorney General Stone banned tapping by the FBI as 'unethical tactics.'"). *But see* Kerr, *supra* note 31, at 843 ("There were sporadic reports of federal agents engaging in wiretapping in the early 1920s."); SMITH, *supra* note 37, at 157 ("[D]iscoveries [of federal wiretapping] were dramatic but not overwhelmingly numerous.").

39. Olmstead v. United States, 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

40. Kerr, *supra* note 31, at 842–43.

41. J. Edgar Hoover, then the director of the Bureau of Investigation within the Department of Justice, told a Congressional committee that he thought that while wiretapping "may not be illegal, I think it is unethical." This did not stop Hoover from using wiretaps and electronic bugs throughout his tenure as director of the FBI. SMITH, *supra* note 37, at 157, 160–75.

42. Kerr, *supra* note 31, at 843–44.

43. *Id.* at 844.

44. *Olmstead*, 277 U.S. at 465. The Court declared that the language of the Fourth Amendment could not be "extended and expanded to include telephone wires, reaching to the whole world from the defendant's home or office, any more than are the highways along which they are stretched." *Id*. Because the officer merely overheard the defendant's conversation, and did not physically enter into the defendant's house or physically search his papers or effects, there was no Fourth Amendment search. *Id*. at 464.

significant, noting that federal criminal cases are controlled by the common law, which does not consider whether evidence was obtained legally in determining whether that evidence is admissible; moreover, because the state statute was not enforced by an exclusionary rule, the statute did not supersede the common law rule.[45]

The Court held that the purpose of the Fourth Amendment was to "prevent the use of governmental force to search a man's house, his person, his papers, and his effects,"[46] and the bare language of the amendment could not be "extended and expanded to include telephone wires."[47] However, the Court also explicitly reminded Congress that the legislative body was not similarly restricted from expanding the scope of the Amendment, and could easily regulate wiretaps by passing legislation prohibiting the use of evidence obtained through wiretapping in federal criminal trials.[48] Despite the Court's clear invitation for statutory review, Congress did not regulate wiretapping until 1934, six years after *Olmstead*.

B. AFTER *OLMSTEAD*: A DIALOGUE BETWEEN CONGRESS, STATE LEGISLATURES, AND THE COURT

A bill to reform the wiretapping regulations was proposed in nearly every congressional session following the Court's 1928 decision in *Olmstead*, but the 1934 Communication Act[49] was the only one successfully enacted.[50] However, "dislike of [the Act] was nearly

45. *Id.* at 466–68. In his dissent, Justice Brandeis suggested that the violation of state law was sufficient to resolve the case; because the evidence underpinning the case against Olmstead was obtained illegally, the "maxim of unclean hands" required that the Court overturn the conviction, or else it would be seen as ratifying the illegal search. *Id.* at 483–84 (Brandeis, J., dissenting).

46. *Id.* at 463.

47. *Id*. at 465.

48. *Id*. at 465–66 ("Congress may, of course, protect the secrecy of telephone messages by making them, when intercepted, inadmissible in evidence in federal criminal trials, by direct legislation, and thus depart from the common law of evidence. But the courts may not adopt such a policy by attributing an enlarged and unusual meaning to the Fourth Amendment.").

49. Communications Act of 1934, ch. 652, 48 Stat. 1064 (current version at 47 U.S.C. § 605 (2000)).

50. Kerr, *supra* note 31, at 847. The 1934 Communication Act stated that "[n]o person, not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person." However, the remedy for violation was unclear, and the Supreme Court subsequently resolved the confusion by interpreting the law to make all wiretapping evidence inadmissible in federal court and later extending "fruit of the poisonous tree" exclusions to information derived from illegal wiretapping. *Id*. at 845.

universal."[51] The law was not well drafted, and the Justice Department interpreted the statute to prohibit only the use of wiretap evidence in court, but not to prohibit the act of wiretapping itself.[52]

Because the Fourth Amendment had not yet been held to apply to the states through incorporation via the Fourteenth Amendment[53] and the 1934 Communication Act only applied to federal prosecutions, independent state regulation of wiretapping continued to develop.[54] By the mid-1960s, there was a pronounced proliferation of state wiretapping regulations; most states had outlawed wiretapping entirely, but some states allowed for some type of authorized use by law enforcement.[55] New York's statute was a representative example, allowing for a judge to issue an "ex parte order for eavesdropping" upon an oath or affirmation stating that "there is reasonable ground to believe that evidence of crime may be thus obtained, and particularly describing the person or persons whose communications . . . are to be overheard or recorded, and the purpose thereof."[56] The order was not to exceed two months, although it could be extended.[57]

In *Berger v. New York*, the Court held New York's wiretap statute to be unconstitutional, but took great care to list the statute's particular constitutional deficiencies.[58] The Court first noted that the statute did not require that the "communications, conversations, or discussions to be seized" be particularly described, only that the subject of the wiretap be identified.[59] Next, the Court objected to the statute effectively authorizing a "series of intrusions, searches, and seizures" over a two-month period on a single showing of probable cause; moreover, it found the "mere showing

51. Solove, *Fourth Amendment Codification*, *supra* note 9, at 770. The Attorney General at the time declared it "the worst of all possible solutions." A later Senate Report associated with the law that would replace the Communication Act stated that the Act "serves . . . neither the interests of privacy nor of law enforcement." Solove, *Reconstructing Electronic Surveillance Law*, *supra* note 17, at 1274–75.

52. The law was seen as both over protective and under protective; unduly constraining law enforcement by prohibiting all wiretap evidence from admission in court, while also failing to protect individuals from government surveillance. Kerr, *supra* note 31, at 846. *Cf.* Solove, *Fourth Amendment Codification*, *supra* note 9, at 770 ("This enabled FBI Director J. Edgar Hoover to wiretap to his heart's content so long as he used wiretapping only to blackmail people, rather than to provide evidence in federal trials.").

53. *See* Mapp v. Ohio, 367 U.S. 643 (1961).

54. Kerr, *supra* note 31, at 846.

55. *Id.*

56. Berger v. New York, 388 U.S. 41, 54 (1967) (quoting N.Y. Code Crim. Proc. § 813-a).

57. *Id.*

58. *Id.* at 54–60.

59. *Id.* at 59.

that [extending the period of eavesdropping] is 'in the public interest'" to be insufficient justification for prolonging the monitoring.[60] The Court also disliked that the statute allowed the wiretap to continue even once the sought-after conversation was seized, based only on the discretion of the officer.[61] Finally, unlike traditional warrants, the statute did not require notifying the individuals involved of the surveillance, nor did it justify this lack of notice by reference to exigent circumstances.[62] The Court recognized that the effectiveness of a wiretap depends on secrecy, but found that a showing of exigency for the eavesdropping is even more essential, as the issuing judge is the only safeguard against abuse.[63]

Lest its holding in *Berger* be interpreted to entirely preclude wiretapping, the Court concluded its opinion by reminding the states and Congress that it had previously allowed use of an "eavesdropping device" when the "'commission of a particular offense' was charged, its use was 'under the most precise and discriminative circumstances,' and the effective administration of justice in a federal court was at stake."[64] After the Court overruled *Olmstead* in *Katz v. United States*,[65] Congress used the standards laid out in *Berger* to craft a comprehensive wiretap standard enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Wiretap Act").[66]

C. BETTER LAWMAKING THROUGH FEDERALISM AND INTER-BRANCH COOPERATION

The Wiretap Act met all of the Court's constitutional requirements for an electronic surveillance statute. The Wiretap Act required that before applying for a court order for a wiretap, prosecutors must first: obtain "high-level" approval from the Justice Department; show that wiretapping will uncover evidence of specific felony offenses; particularly describe the nature and location where the communication will be intercepted, and the

60. *Id.*

61. *Id.*

62. *Id.* at 60.

63. *Id.*

64. *Id.* at 63. *See also* Kerr, *supra* note 31, at 849 ("[T]he major constitutional decisions in *Berger* and *Katz* were carefully timed to influence the shape of statutory law.").

65. *See* Katz v. United States, 389 U.S. 347, 353 (1967) ("We conclude that the underpinnings of *Olmstead* . . . have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling.").

66. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, § 802, 82 Stat. 212 (current version at 18 U.S.C. §§ 2510–2520 (2013)).

identity of the persons who will be so communicating, if known; show that exigent circumstances require use of a wiretap; offer the facts behind all prior wiretap applications; show probable cause that interception of the conversation will yield evidence concerning the sought-after offense; explain the steps taken to minimize interception of unrelated communications.[67] Furthermore, the government must file "regular reports" with the issuing judge justifying the need for further wiretapping, which must not last longer than thirty days in any event.[68] Finally, within ninety days of the end of surveillance, the subject of the wiretap must be informed of the fact they were tapped and when the wiretapping occurred.[69]

Although the Wiretap Act has gaps and weaknesses,[70] the Court has largely declined to make any judicial alterations to the statute.[71] Congress created a comprehensive legislative scheme that met the guidelines laid out in *Berger*, and the Court's subsequent jurisprudence has involved statutory, rather than constitutional, interpretation.

Thirty-four years elapsed between Congress's first failed attempt to regulate wiretapping and the creation of the enduring statutory scheme encompassed in the Wiretap Act. Over that time, Congress, the Court, and state legislatures all had a role in developing the legislation. Congress used *Berger* and *Katz* as a "guide in drafting [the Wiretap Act]," thereby addressing the failings of New York's legislation in the federal statute.[72] Moreover, in the years after the passage of the Wiretap Act, many states

67. Kerr, *supra* note 31, at 851.

68. *Id.*

69. *Id.* at 852.

70. *See* Sklansky, *supra* note 5, at 203. For example, the Act did not initially cover the interception of communications between cordless telephones and the base station. *Id.* With courts reluctant to modify the Wiretap Act, the issue was not resolved until 1994, when Congress "statutorily prohibit[ed] warrantless interception of conversations carried out on cordless telephones." *Id.*

71. Kerr, *supra* note 31, at 852–53. The Court has recognized that, with regards to wiretapping, "Congress did not leave it to the courts to develop a body of Fourth Amendment case law governing that complex subject. . . . Instead, Congress promptly enacted a comprehensive statute and since that time, the regulation of wiretapping has been governed primarily by statute and not by case law." United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring). Kerr also noted that lower courts have been sensitive to Congress' authority in regulating wiretaps. *See, e.g.*, United States v. McNulty, 47 F.3d 100, 105–06 (4th Cir. 1995) ("Congress undertook in Title III to legislate comprehensively in this field and has shown no reluctance to revisit it. Accordingly, we must decline . . . to usher in through the Fourth Amendment a prohibition of that which . . . Congress affirmatively permitted at the time this case arose.").

72. Solove, *Reconstructing Electronic Surveillance Law*, *supra* note 17, at 1275.

have crafted their own wiretap statutes that adhere quite closely to the federal wiretapping law.[73]

Although the process did not happen quickly, the Court, Congress, and state legislatures all contributed to the creation of the Wiretap Act, legislation that addressed an important societal need and which has endured for nearly fifty years without significant revision.[74] Regrettably, the collaborative efforts that led to the Wiretap Act have not been directed at modern electronic communications. In particular, the Court has been unable to coherently determine constitutional limits on surveillance, even as developing technology continues to "shrink the realm of guaranteed privacy."[75] The following Section shall examine one of the sources of the Court's difficulties.

III. "*KATZ* CRADLE": THE COURT'S TANGLED REASONABLENESS ANALYSIS

A. LINGUISTICS AND INSTITUTIONAL COMPETENCE

The Fourth Amendment prohibits "unreasonable searches and seizures."[76] "Unreasonableness" may be seen as an archetypical example of an "extravagantly vague" term, a term that is characterized by requiring "a *multidimensional* evaluation [between] *incommensurable* constitutive elements."[77] The judiciary is institutionally oriented towards this sort of

73. *Cf.* ROBERT ELLIS SMITH, PRIVACY JOURNAL'S COMPILATION OF STATE AND FEDERAL PRIVACY LAWS (2012). For example, California, Connecticut, Delaware, Florida, Hawaii, Illinois, Louisiana, Maryland, Massachusetts, Montana, New Hampshire, Oregon, Pennsylvania, and Washington require two-party consent for recording, while the Wiretap Act only requires one-party consent. Pennsylvania is the only state that has dramatically superseded the federal law by forbidding any wiretapping or eavesdropping, *even by law enforcement*, without the consent of both parties. *Id*.

74. Since passing the Wiretap Act, Congress has addressed electronic surveillance in two other major statutes, the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 (2013) and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107-56, 115 Stat. 272 (codified as amended in scattered sections of 8 U.S.C., 15 U.S.C., 18 U.S.C., 31 U.S.C., 42 U.S.C., 49 U.S.C., 50 U.S.C.). The later legislation created a broad legislative framework for surveillance of electronic communication, and although the statutory scheme provided relatively weak protection for electronic communications such as email, it largely maintained the strong protections of wiretaps required by the Wiretap Act. *See* Solove, *Reconstructing Electronic Surveillance Law*, *supra* note 17, at 1277–78.

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

76. 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.").

77. Andrei Marmor, *Varieties of Vagueness in the Law* 1–4 (USC Legal Studies Research Paper No. 12, 2013) (emphasis in original), *available at* http://ssrn.com/abstract=2039076. The author cites

evaluation and is often called upon by the legislature or by the Constitution to find some sort of balance between asymmetrical factors.[78]

Furthermore, while "search" is also a vague term because it is not necessarily obvious whether some action constitutes a "search" or not, it is merely an ordinarily (or "transparently") vague word no different than any other linguistically non-specific word.[79] Whereas the judiciary is particularly suited to analysis of extravagantly vague terms like "unreasonable," other branches of government are equally capable of defining the scope of transparently vague terms.[80]

In *Olmstead*, the Court weighed whether the traditional scope of Fourth Amendment protections, which the Court interpreted as barring the government from trespassing on private property or searching for physical items, should be expanded to include non-tangible telephone conversations gathered without trespass into an individual's home.[81] The Court did not address whether the government acted reasonably in listening to Olmstead's telephone conversations, but simply determined that a "search" has not occurred when the government has not trespassed on private property, nor searched any tangible possessions.[82] By assessing whether the challenged actions constituted a "search" and not whether the action was

"neglect" as another example of an extravagantly vague term; laws prohibiting child abuse require courts to weigh whether, for example, it is worse to neglect a two-year-old child for ten minutes or a six-year-old child for two hours, and to consider a multitude of other relevant factors when assessing culpability. *Id.*

78. Legislation concerning these sorts of topics will often include an extravagantly vague term as an invitation for judicial review, although it will commonly include a number of explicit examples of the class. *Id.* This allows "the courts to form a holistic, all-things-considered judgment of the particular case at hand . . . [and to] have some specific rules that are aimed to shape such decisions and determine, in advance, some of the conditions that the relevant conduct has to meet." *Id.* at 18.

79. *Id.* at 2–3. Linguistically vague terms typically imply a "sorities" sequence, in which some examples of the term are universally accepted as being included in the term, while some fringe examples may or may not be included. For example, individuals over six foot five inches are clearly "tall," while people who are five foot eleven inches may or may not be "tall." Likewise, a search has clearly occurred when the government enters a suspect's house to find evidence of a crime, but may or may not have occurred when a government agent looks in a suspect's window.

80. *Id.* at 15–16. However, just because the Court is suited to defining "unreasonableness" does not mean that it has done so consistently; the Court's earlier reasonableness analysis has been inconsistent and has not provided strong protection against government intrusion. Solove, *Reconstructing Electronic Surveillance Law*, *supra* note 17, at 1302–03.

81. Olmstead v. United States, 277 U.S. 438, 463 (1928) ("The well-known historical purpose of the Fourth Amendment . . . was to prevent the use of governmental force to search of a man's house, his person, his papers and his effects.").

82. *Id.* at 464.

"unreasonable," the Court focused on a transparently vague term; thus, its decision in this case was due minimal institutional deference (and was expressly overruled in *Katz*).[83]

Justice Brandeis's dissent in *Olmstead* highlighted the mistaken focus of the Court's analysis. In an opinion beginning with a quote from *McCulloch v. Maryland*,[84] Justice Brandeis proceeded to declare that a wiretap is an *unreasonable* search, writing that:

> [T]he evil incident to invasion of the privacy of the telephone is far greater than that involved with tapering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them on any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of every other person who he may call or whom may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire-tapping. . . . [Because the Founders] conferred, as against the government, the right to be let alone . . . every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.[85]

Although Justice Brandeis's dissent in *Olmstead* set forth the broad outlines of a uniquely judicial analysis of the Fourth Amendment, his opinion has had little impact on the Court's subsequent analysis of the Fourth Amendment. When *Olmstead* eventually became "eroded by . . . subsequent decisions" and was overturned in *Katz*, the *Katz* majority did not cite to Justice Brandeis's *Olmstead* dissent.[86] Moreover, while the *Katz* majority opinion took some steps towards making a uniquely judicial Fourth Amendment analysis, the lasting impact of *Katz* has been in Justice Harlan's concurrence, an opinion that advocated a non-judicial, evidentiary resolution to Fourth Amendment claims.

83. This institutional uncertainty may further explain the Court's invitation to Congress to legislate an exception to the "common law of evidence" and make wiretapping evidence excluded from criminal trials. *Id.* at 465–66.

84. McCulloch v. Maryland, 17 U.S. 316, 407 (1819) ("We must never forget that it is a Constitution we are expounding.").

85. *Olmstead*, 277 U.S. at 475–76, 478 (Brandeis, J., dissenting).

86. Katz v. United States, 389 U.S. 347, 353 (1967).

B. REASSESSING "UNREASONABLE" SEARCHES

1. Katz v. United States

When FBI agents attached a microphone to the outside of a public telephone booth and recorded Charles Katz transmitting gambling information across state lines, the surveillance was not abusive or egregious.[87] The agents had established a "strong probability" that the recording would contain evidence of illegal activities and took "great care to overhear only the conversations of [the suspect] himself."[88] Moreover, because the placement of the microphone "involved no physical penetration of the telephone booth from which the petitioner placed his calls," it did not constitute a search under the trespass-oriented standard the Court articulated in *Olmstead*.[89] The government asserted that "its agents acted in an entirely defensible manner."[90]

The Court rejected the government's arguments and repudiated *Olmstead*. In holding that "[t]he Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth," the Court properly assessed whether the government's actions were reasonable.[91] The Court declared that an individual is "surely entitled to assume" that discussions in a public telephone booth would not be "broadcast to the world," just the same as if the conversation occurred in a home or office.[92] In its reasonableness analysis, the Court weighed various incommensurable elements including: Katz being in a public place; being visible to the public, but inside an enclosed telephone booth; the "vital role" the public telephone plays in private communication; his intention to exclude "the uninvited ear" by entering the booth and closing the door; and the lack of judicial restraint on the government compared to what would be imposed through a warrant.[93]

Stating that the "Fourth Amendment protects people, not places" and that what a person "seeks to preserve as private, even in an area accessible

87. *Id.* at 356.

88. *Id.* at 354.

89. *Id.* at 352–53. Recall that *Olmstead* held that a "search" does not occur without trespass on a constitutionally protected area. *Olmstead*, 277 U.S. at 466.

90. *Katz*, 389 U.S. at 354.

91. *Id.* at 353.

92. *Id.* at 352–56.

93. *Id.*

to the public, may be constitutionally protected," the Court expanded the scope of its Fourth Amendment analysis beyond simply determining whether a trespass occurred.[94] *Katz* reoriented the Court towards its proper object in constitutional analysis: by focusing on whether the government's actions were reasonable, not whether the actions constituted a search, the Court returned to interpreting the scope of "extravagantly vague" terms rather than those that were merely "linguistically" vague.[95]

2. Justice Harlan's Misstated Concurrence

Although *Katz* is the controlling standard for most subsequent Fourth Amendment cases, it is Justice Harlan's concurrence that these cases typically cite.[96] Justice Harlan examined the Court's Fourth Amendment jurisprudence and concluded that "[m]y understanding of the rule that has emerged from prior decisions is that there is a twofold requirement [for Fourth Amendment protection], first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[97]

Yet, Justice Harlan's restatement of the Court's Fourth Amendment history is not identical to the reasonableness analysis described by the *Katz* majority. There is a significant difference between determining if a search is "unreasonable" and determining whether society accepts some action as reasonable or unreasonable. In the former case, the term is extravagantly vague and is best analyzed by the judiciary. In the latter case, the analysis is largely an evidentiary problem; "society" is merely a linguistically vague term, capable of statutory definition; therefore, legislatures are equally capable of determining the privacy expectations that "society accepts as reasonable."[98] Slobogin suggests that this non-judicial evidentiary

94. *Id.* at 351–52.

95. *But see* Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 325–27 (1998) (arguing that *Katz* was a narrow decision, "extending the protections of the amendment only to intangible interests such as phone conversations" and did not adopt the "broad-based philosophical argument" of Justice Brandeis's dissent in *Olmstead*).

96. *See* United States v. Jones, 132 S. Ct. 945, 950 (2012) ("Our later cases have applied the analysis of Justice Harlan's concurrence in [*Katz*], which said that a violation occurs when government officers violate a person's 'reasonable expectation of privacy.'"); Kyllo v. United States, 533 U.S. 27, 33 (2001).

97. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

98. Henry F. Fradella et al., *Quantifying Katz: Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289, 293 (2011) ("[A] significant problem with *Katz* is that the Court has never attempted to determine in any systematic way how "society" might objectively view privacy rights in a particular search and seizure context, even

emphasis indicates that the Court did not intend the *Katz* test to be read literally, and that doing so "render[s] nugatory the language and history of the Fourth Amendment."[99] However, this saving interpretation does not reflect the Court's analysis of subsequent Fourth Amendment cases.[100]

While the Court usually cites *Katz* as the foundation of its analysis of the reasonableness of the search, by citing to Justice Harlan's concurrence the Court may be substituting a judicial analysis for one more properly delegated to the legislature; this may be one of the reasons the Court's Fourth Amendment jurisprudence has been inconsistent and variable.[101] Moreover, as the *Katz* test requires the Court to assess the privacy expectations that "society is prepared to recognize as reasonable," the Court must therefore find some evidence of what "society" feels is a reasonable expectation of privacy. This evidentiary difficulty presents another challenge to the Court's Fourth Amendment analysis and shall be examined in greater detail in the following sections.

C. *KYLLO* AND *JONES*: EVIDENCE OF SOCIALLY ACCEPTED PRIVACY EXPECTATIONS

Justice Harlan's dual-pronged expectation-of-privacy test implies an evidentiary problem: how can the Court know what particular subjective expectations of privacy society believes are reasonable? Two recent cases, both with a majority opinion written by Justice Scalia, illustrate the difficulties the Court has in determining how developing technology changes Fourth Amendment privacy rights.

1. Kyllo v. United States

Kyllo presented the Court with an opportunity to determine the limits on the "power of technology to shrink the realm of guaranteed privacy."[102] In *Kyllo*, a Department of the Interior agent suspected that marijuana was

though the rationale of *Katz* explicitly rest on such societal judgments. *Katz*, therefore, invites scrutiny of the legitimacy of judicial decision-making.").

99. CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 114–15 (2007).

100. *See infra* Section III.C.

101. *See, e.g.*, Clancy, *supra* note 95, at 344 ("The most important and fundamental flaw in the Court's reliance on privacy analysis is that the inquiry has abandoned the structure of the Fourth Amendment and is based on confusing motivation for exercising the right to be secure with the right itself."); Solove, *Fourth Amendment Pragmatism*, *supra* note 7, at 1511 ("The reasonable expectation of privacy test has led to a contentious jurisprudence that is riddled with inconsistency and incoherence.").

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

being grown in one unit in a triplex.[103] In investigating the case, the agent used an "Agema Thermovision 210" thermal imager to discover that the suspect's garage was "relatively hot" compared to the rest of the house and the neighboring units.[104] Based on this evidence, along with utility bills and informant information, agents obtained a search warrant and discovered a large marijuana growing operation.[105] No state or federal laws regulated use of thermal imaging devices by law enforcement, and the Court had previously "reserved judgment" on the threshold beyond which technology enhanced "ordinary perception . . . too much" and began to infringe Fourth Amendment rights.[106]

Justice Scalia begins the majority opinion by reiterating the two-prong privacy standard set forth in Justice Harlan's concurrence in *Katz*,[107] although he notes that the *Katz* test "has often been criticized as circular, and hence subjective and unpredictable."[108]

He continues by finding that both prongs of the test are inherent in basic, common law principles; the historical common law protection of the "interior of homes" demonstrates both an essential "minimal expectation of privacy that *exists*, and that is acknowledged [by society] to be *reasonable*."[109] While the analysis is not explicit, Justice Scalia presumably means that homeowners have a subjective expectation of privacy in their homes (and that the expectation of privacy extends to a privacy interest in the external temperature of the house), and that society finds this subjective expectation reasonable.[110]

103. *Id.* at 30.

104. *Id.* The lights used to grow marijuana indoors are quite hot, so the relative warmth of the garage indicated that marijuana was possibly being grown there.

105. *Id.*

106. *Id.* at 33.

107. A search occurs when "a person [has] exhibited an actual (subjective) expectation of privacy and . . . the expectation [is] one that society is prepared to recognize as 'reasonable.'" United States v. Katz, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

108. *Kyllo*, 533 U.S. at 34. Moreover, he suggests that later cases have applied the test "somewhat in reverse"; rather than the test being one of many potentially *sufficient* standards to determine whether a search occurred, Justice Scalia suggests that satisfying Justice Harlan's two-prong test is a *necessary* prerequisite for a search to have occurred. *Id*. at 33 ("We have subsequently applied this principle to hold that a search does *not* occur . . . unless 'the individual manifested a subjective expectation of privacy in the object of the challenged search,' and 'society [is] willing to recognize that exception as reasonable.'").

109. *Id.* at 34 (emphasis in original).

110. *See id.*

a. Evidentiary Objections

Whether this syllogism is valid seems to depend on the extent and quality of the common law protections of the home, and whether society continues to recognize those common law standards as reasonable. Justice Scalia writes that "the Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained."[111] This suggests that he believes that the Fourth Amendment protects virtually all intrusions into the home, and such intrusions are *per se* unreasonable and require that a warrant be obtained prior to the search.[112] Justice Scalia gives further weight to this principled approach to privacy rights by highlighting the importance of crafting an expansive rule that "take[s] account of more sophisticated systems that are already in use or in development."[113] These statements imply a broad "reasonableness" analysis that assesses the impact of technological developments without appreciable reference to the specific rights historically granted by the common law.[114] In suggesting that an unreasonable search occurs when any "sense-enhancing technology" is used to obtain information about the interior of a home, he describes a uniquely judicial project that requires judgment regarding: whether a particular device is a "sense-enhancing technology"; whether that device obtained information about the "interior" of a "home"; and whether the information could have been otherwise obtained.

However, Justice Scalia's opinion does not resolve the tension between an evidentiary approach to privacy interests and a judicial analysis of an "extravagantly vague" privacy interest. By comparing the privacy

111. *Kyllo*, 533 U.S. at 37.

112. *Id.*

113. *Id.* at 36.

114. *Cf.* Smith v. Maryland, 422 U.S. 735, 743–45 (1979) (holding that the installation and use of "pen registers," devices which record the telephone numbers dialed by a particular telephone customer, was not a "search," and no warrant was required). The Court held that the customer did not have a reasonable expectation that the phone numbers dialed on a private telephone would remain private because the numbers were clearly transmitted to the telephone company and previous cases have consistently held that an individual "has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* Moreover, since "petitioner concede[d] that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy . . . [the Court is] not inclined to hold that a different constitutional result is required because the telephone company has decided to automate." *Id.* The analysis was not based on an assessment of common law, but rather judicial consideration of the reasonableness of a particular individual's expectation of privacy in a certain situation. *Id.*

right in *Kyllo* with historical common law privacy rights, and seeking to "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted," Justice Scalia's argument seems vulnerable to contrary historical data.[115] Indeed, the dissent makes the evidentiary charge that Justice Scalia's opinion is mistaken because "the chief evil against which the wording of the Fourth Amendment is directed" is the "physical entry of the home" and not the public appearance or characteristics thereof, therefore gaining information about the interior of a home without physical entry does not constitute a search.[116] Analysis of historical common law protections is not an exclusively judicial project; the legislature is at least as qualified to resolve this sort of evidentiary dispute, if not more so.[117]

Moreover, Justice Scalia concludes 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 . . . the technology in question is not in general public use."[118] This final caveat that the technology must not be in common use seems to make the Fourth Amendment analysis envisioned in *Kyllo* an evidentiary matter; if some technology is in "general public use," then Justice Scalia seems to suggest that information obtained thereby would not be entitled to Fourth Amendment protections.[119] This final qualification subverts the opinion, and seems to require the Court to take judicial notice of such evidence as

115. *Id.* As with many originalist analyses of Constitutional issues, there is scholarly disagreement on the finer points of the Founder's intent. *Compare* Steinberg, *supra* note 32, at 583 (stating that "[h]istorical sources indicate that the Framers were focused on a single, narrow problem: physical trespasses into houses by government agents," so the Fourth Amendment is inapplicable outside of house searches), *with* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 551, 556 (1999) (arguing that the purpose of the Fourth Amendment was "banning Congress from authorizing use of general warrants" although strictly adhering to that original understanding "would subvert the purpose the Framers had in mind when they adopted the text").

116. *Kyllo*, 533 U.S. at 46 (Stevens, J., dissenting).

117. *See* Kerr, *supra* note 31, at 867–70 (describing the institutional advantages of legislative *ex ante* rulemaking).

118. *Kyllo*, 533 U.S. at 34.

119. Moreover, the requirement seems to negate the Court's goal in crafting a rule that accounts for further technological developments. *See id.* at 47 (Stevens, J., dissenting) ("[T]he contours of [the Court's] new rule are uncertain because its protection apparently dissipates as soon as the relevant technology is "in general public use." . . . [T]his criterion is somewhat 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.").

sales figures, availability of stock, and other objective data to determine whether some technology is in general use or not.

A similar confusion is present in the Court's next significant case addressing the Fourth Amendment implications of technological development, *United States v. Jones*.

2. United States v. Jones

Although the conclusion in *Jones* was unanimous, Justices Scalia, Sotomayor, and Alito each wrote opinions with widely differing reasoning.

Antoine Jones, a Washington, D.C. nightclub owner, was being investigated by the FBI for drug trafficking.[120] Acting under an expired warrant, agents placed a GPS tracking device on the undercarriage of a vehicle used by Jones and tracked the vehicle for the next twenty-eight days, generating two thousand pages of data for the time period in question.[121] Based on the GPS evidence, agents obtained a grand jury indictment of Jones, who was eventually found guilty and sentenced to life imprisonment.[122] The Court granted certiorari to determine whether use of evidence obtained by a warrantless GPS device violated the Fourth Amendment.[123]

a. Majority (Scalia)

Justice Scalia's majority opinion in *Kyllo* described the common law privacy interest in the "interior of homes." In *Jones*, Justice Scalia writes that a similar common law privacy interest prevents government agents from physically trespassing on private property to obtain information about the owner of that property. He asserts that historically, "the Fourth Amendment was understood to embody a particular concern for government trespass upon [enumerated] areas"[124] and notes that "Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the twentieth century."[125] Although the *Katz* "reasonable-expectation-of-privacy test" had been widely accepted as supplanting this

120. United States v. Jones, 132 S. Ct. 945, 948 (2012).
121. *Id.*
122. *Id.*
123. *Id.* at 949.
124. *Id.* at 950.
125. *Id.* at 949.

property-based approach to privacy interests,[126] Justice Scalia declared that the *Katz* test was merely "*added to*, not *substituted for*, the common-law trespassory test"; when the government makes non-trespassory surveillance of electronic signals, the surveillance remains subject to the *Katz* analysis.[127]

Notwithstanding Justice Scalia's endorsement of a trespass-based privacy standard which many had thought was overruled by *Katz*, he does not argue that all government trespass constitutes a Fourth Amendment search; rather, the government committed a search when it installed the GPS device *and* used the device to obtain information.[128] In placing the GPS device, the government "physically occupied private property for the purpose of obtaining information," and thereby committed an unreasonable search under the original meaning of the Fourth Amendment.[129] Justice Scalia finds that this new trespass-oriented two-prong test provides a level of protection consistent with "an 18th-century guarantee against unreasonable searches," which he understands to be the minimum level of protection required by the Fourth Amendment.[130]

b. Concurrence (Alito)

Justice Alito, along with many of the Court's liberal justices, concurred in the majority's judgment but based his analysis on the *Katz* reasonable-expectation-of-privacy test.[131] However, Justice Alito finds only the long-term GPS tracking of Jones to be impermissible government action and does not find that the attachment of the GPS device itself

126. *See* United States v. Katz, 389 U.S. 347, 353 (1967) ("We conclude that . . . the 'trespass' doctrine . . . can no longer be regarded as controlling."); United States v. Karo, 468 U.S. 705, 713 ("[A]ctual trespass is neither necessary *nor sufficient* to establish a constitutional violation."); Clancy, *supra* note 95, at 328 (stating that *Katz* has come to stand for the narrow principle that "property interests do not control the determination of whether a search of seizure has occurred").

127. United States v. Jones, 132 S. Ct. 945, 952 (2012) (emphasis in original). *See also* Clancy, *supra* note 95, at 360 (suggesting that the trespass-based theory of privacy in *Olmstead* protected the right to exclude, which was properly extended in *Katz* to prevent "non-physical invasions of intangible objects").

128. *Jones*, 132 S. Ct. at 949. *See also id*. at 951, n.5 ("Trespass alone does not qualify, but . . . must be conjoined with . . . an attempt to find something or to obtain information.").

129. *Id.* at 949.

130. *Id.* at 953.

131. Justice Alito notes that although *Katz* is not an ideal test, involving "a degree of circularity" and containing the risk that "judges [will] . . . confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks," it is a superior standard compared to the trespass-test put forward by the majority. *Id*. at 962 (Alito, J., concurring).

constituted a search because the attachment was not a "meaningful interference with an individual's possessory interest[] in [the] property."[132]

Justice Alito begins by criticizing the majority for reviving a trespass-based standard that is in "disharmony" with the Court's post-*Katz* jurisprudence.[133] He proceeds to point out a number of instances in which the majority's trespass standard would provide insufficiently robust protections compared to the *Katz* standard or would lead to inconsistent results; if, for example, the government could accomplish the same long-term GPS tracking without physical trespass, the subject of that surveillance would have no protection under the majority's approach.[134]

Justice Alito's opinion is notable for two reasons. First, he recognizes that technological advances may well lead to a reduced expectation of privacy when the technological benefits provide "increased convenience or security at the expense of privacy."[135] While making this observation, he also asserts *de facto* limitations on the extent of surveillance society may accept as reasonable. Without offering any basis for his assertions, he suggests that as an outer bound, GPS tracking of a vehicle for twenty-eight days is "surely" an unreasonable search, while "relatively short-term monitoring" of an individual on public streets accords with accepted expectations of privacy.[136] This aspect of Justice Alito's opinion suggests that even those Justices most supportive of the *Katz* test have difficulty applying a standard that predicates privacy rights upon evidence of socially accepted practices; in setting an outer bound after which surveillance is "surely" unreasonable, Justice Alito implies the Court ought to do more than simply determine societal expectations.[137]

Second, Justice Alito makes the contrary assertion that the Court may not have a role in determining privacy interests at all. Given the rapid pace of technological advancements, and the significant impact of those changes upon society, he writes that "the best solution to privacy concerns may be legislative."[138] Although he notes that the legislature has not acted to

132. *Id.* at 958.

133. *Id.* at 961.

134. *Id.* at 961–62.

135. *Id.* at 962. Moreover, the *Katz* test may not find a protectable privacy interest "even if the public does not welcome the diminution of privacy that new technology entails." *Id.*

136. *Id.* at 964.

137. *See id.*

138. *Id.*

regulate GPS technology, Justice Alito suggests that "[a] legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[139] Justice Sotomayor echoes this sentiment in her separate concurring opinion.

c. Concurrence (Sotomayor)

Justice Sotomayor joined the majority opinion, agreeing that the trespass-based test, which provides an "irreducible constitutional minimum" of protection against search and seizure, is sufficient to resolve the specific issues presented in *Jones*.[140] However, she also writes a separate concurrence in which she indicates her agreement with Justice Alito that the *Katz* test is an appropriate framework for assessing the privacy implications of developing surveillance technology.[141]

Justice Sotomayor's concurrence expresses a more expansive approach to privacy issues than either Justice Scalia's majority or Justice Alito's concurrence.[142] She is the only Justice to suggest that even a short period of GPS monitoring constitutes a search, and she suggests that the government's ability to obtain "at a relatively low cost such a substantial quantum of intimate information about any person" requires modifying the typical application of the *Katz* test.[143]

Typically, the Court's *Katz* analysis has focused on whether the expressed expectation of privacy was accepted by society as reasonable and has presumed that an individual has demonstrated a subjective expectation of privacy in whatever information he has not exposed to the public.[144]

139. *Id. See also* Kerr, *supra* note 31, at 857–82 (generally arguing that legislatures are better able to respond to the Fourth Amendment implications of technological change); City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010) ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.").

140. United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring).

141. *Id.*

142. Tom Goldstein, *Reactions to Jones v. United States: The Government Fared Much Better than Everyone Realizes*, SCOTUSBLOG (Jan. 23, 2012, 4:07 PM), http://www.scotusblog.com/2012/01/reactions-to-jones-v-united-states-the-government-fared-much-better-than-everyone-realizes.

143. *Jones*, 132 S. Ct. at 955–56 (Sotomayor, J., concurring). *See also* Tom Goldstein, *Why Jones is Still Less of a Pro-privacy Decision than Most Thought (Conclusion slightly revised Jan. 31)*, SCOTUSBLOG (Jan. 30, 2012, 10:53 AM), http://www.scotusblog.com/2012/01/why-jones-is-still-less-of-a-pro-privacy-decision-than-most-thought.

144. One notable exception is Smith v. Maryland, 442 U.S. 735, 743–44 (1975), in which the Court held that an individual has not exhibited an actual expectation of privacy in telephone numbers dialed from a home telephone when the numbers are obviously transmitted to the telephone company.

Justice Sotomayor writes that because GPS monitoring "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious and sexual associations," an individual may have a privacy interest in the aggregated information even if it is otherwise publicly available.[145] Prior applications of *Katz* have held that society does not find such expectations reasonable and have found that an individual's subjective expectation of privacy is not valid if the information has been exposed to the public.[146] Justice Sotomayor indicates her willingness to reconsider whether "to treat secrecy as a prerequisite for privacy" and whether an individual may retain an expectation of privacy in information that has been voluntarily disclosed to a third party.[147]

Further, Justice Sotomayor offers a prudential reason to expand the *Katz* test: awareness of government surveillance may hamper individual exercise of "associational and expressive freedoms."[148] Whereas Justice Alito suggested that Congress may be better suited to assess the privacy implications of technological development than the Court, Justice Sotomayor writes that legislative or judicial oversight of electronic surveillance may be needed as a check on the executive branch; electronic surveillance, particularly the use of GPS and cellular telephone data, is a "a tool so amenable to misuse" that the legislature or judiciary should have a role in supervising and regulating executive use of such surveillance.[149]

Justice Sotomayor's concurrence is a significant development in the Court's Fourth Amendment jurisprudence. Her suggestion that individuals may have an expectation of privacy in certain information, "whatever the societal expectations," may signal that the subjective-expectation-of-privacy prong of the *Katz* test will be given greater weight in the future.[150] At minimum, at least one Justice recognizes that substantial technological change may require similarly substantial changes in the Court's analysis of privacy.

145. *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).

146. *See* California v. Ciraolo, 476 U.S. 207, 215 (1986) (holding that society does not accept a subjective expectation of privacy in a back yard viewed from above, when airplanes may legally travel over the back yard); California v. Greenwood, 486 U.S. 35, 39–41 (1988) (holding that society does not accept a subjective expectation of privacy in trash left on the curb for collection).

147. *Jones*, 389 U.S. at 957 (Sotomayor, J., concurring).

148. *Id.* at 956.

149. *Id*.

150. *Id.*

3. Is the Court Allergic to Katz?

In both *Kyllo* and *Jones*, the Court clearly struggles with placing limits upon the "power of technology to shrink the realm of guaranteed privacy."[151] In both cases, Justice Scalia shows little tolerance for the *Katz* test, and generally tries to return Fourth Amendment jurisprudence to the trespass-based standard of *Olmstead* and the common law. While Justice Scalia pays some lip service to the *Katz* two-prong test, he avoids actually applying the test by using common law trespass principles to satisfy both prongs.[152]

Insofar as the Court is somewhat better suited to assess the application of the common law than it is to determine socially accepted expectations of privacy, Justice Scalia's common law gloss on the *Katz* test may provide some consistency in the Court's Fourth Amendment jurisprudence. However, the common law may not provide accurate evidence of societal expectations.

a. Common Law Evidence of Societal Expectations of Privacy

In *Kyllo* and *Jones*, Justice Scalia suggested that the common law might be a repository of societal information regarding subjective expectations of privacy that are inherently accepted as reasonable by society.[153] In these cases, the Court articulated two common law rights that are closely linked to Fourth Amendment protections: one protecting information about the interior of homes not otherwise available without physical intrusion and the other preventing the government from physically occupying private property for the purpose of gathering information.[154] However, the articulations of these common law principles may not be

151. Kyllo v. United States, 553 U.S. 27, 34 (2001).

152. *Id.*

153. Substantial objections have been made to this suggestion. Various scholars have charged that: society has changed too dramatically to adhere to 18th-century search and seizure practices (and moreover that such adherence would subvert the purpose of the Fourth Amendment); a common-law analysis is inherently incomplete and indeterminate, allowing partisan or ideological decisions to be made under the guise of objective analysis; because the Framers did not consider issues of "race, class, and gender," a historical approach to the Fourth Amendment may overlook equality concerns. S*ee, e.g.*, Cynthia Lee, *Reasonableness with Teeth: The Future of Fourth Amendment Reasonableness Analysis*, 81 MISS. L.J. 1133, 1143–46 (2012). *But see* Sklansky, *supra* note 5, at 185–88, suggesting that the Court's historical perspective is not a strictly originalist inquiry into the content of 18th-century search and seizure law, but is rather a holistic declaration of the traditional scope of Fourth Amendment doctrine, emphasizing not the actual content of the law in the eighteenth century, but rather what the law "came to understand itself as doing."

154. *See supra* Section III.C.

based on "expectations of privacy and autonomy [that] reflect realistic societal attitudes" but rather on the privacy assessments and expectations of individual judges and Justices.[155]

If the common law principles reflect only the societal values of the Court, they may not constitute accurate evidence of societal privacy expectations, especially as those expectations change in response to technological innovation.[156] However, the Court's recourse to common law privacy protections may be justified if those decisions using common law evidence broadly reflect social privacy expectations. If an empirical analysis of privacy expectations roughly correlates with the Court's decisions, this may suggest that the common law is a legitimate indicator of societal privacy expectations.

b. Empirical Evidence of Privacy Expectations[157]

Although only a few broad empirical studies of privacy expectations have been conducted, they reveal some societal expectations at odds with the Court's jurisprudence.[158] The studies suggest that "courts often misjudge what 'society' is prepared to embrace as a reasonable expectation of privacy."[159]

The most comprehensive of these studies occurred in 2011 and assessed the privacy expectations of 549 individuals from varying

155. Christopher Slobogin, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society"*, 42 DUKE L.J. 727, 775 (1993). *See also* Fradella et al., *supra* note 98, at 293–94 (suggesting that the Court makes "no attempt to discern actual societal opinions when adjudicating Fourth Amendment disputes," and that common law principles are no more than the "suppositions that thoughtful reflection can provide").

156. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring) ("[J]udges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the Katz test looks. In addition, . . . [d]ramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes.")

157. It should be emphasized that the empirical information referenced below is simply put forward as a way to gauge the accuracy of the Court's assessment of the expectations of privacy that society accepts as reasonable, and not that the Court should embrace empirical data as defining societal expectations. *See* DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 117 (2011) ("Following polls and surveys would shackle the Fourth Amendment to the preferences of the majority. Minority groups may have different attitudes about privacy.").

158. *See, e.g.*, Jeremy A. Blumenthal et. al., *The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy"*, 11 U. PA. J. CONST. L. 331, 341 (2009); Fradella et al., *supra* note 98, at 293; Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 S. ILL. U. L.J. 475, 522 (2012).

159. Fradella et al., *supra* note 98, at 372.

backgrounds.[160] The study found that respondents expressed "significant levels of agreement" with Court decisions upholding privacy rights, but also expressed significant disagreement with decisions rejecting privacy rights.[161]

For example, 60% of the respondents to the study agreed with the holding in *Kyllo* that an individual has a reasonable expectation of privacy in the heat emanating from his or her home, while 24% disagreed.[162] The rate of approval for *Katz* was even greater, with 63.1% of respondents agreeing that a warrant should be required to record a phone conversation, while 23.1% disagreed.[163] On the other hand, respondents to the study generally disagreed with those decisions that failed to uphold a privacy interest, particularly when the decision concerned electronic surveillance.[164] Although the study was conducted prior to the decision in *Jones*, 85.5% of respondents disagreed with the conclusion in *United States v. Knotts*,[165] which found that individuals had no reasonable expectation of privacy while traveling along public roads, and further held that tracking of vehicles through the use of "beepers," a precursor to GPS, did not constitute a Fourth Amendment search.[166] A similar percentage of

160. *Id.* at 346. The study found no differences in privacy expectations based on race, religion, or sex, suggesting that there are some privacy expectations that society as a whole, and not just a given demographic group, accepts as reasonable. *Id.* at 370–71.

161. *Id.* at 362–67 (noting that there were a number of instances in which respondents did not feel that some government action impinged a privacy right and did not express a clear expectation of privacy in that activity, including: warrantless seizure of blood samples from DUI suspects; search of a vehicle's passenger if the officer has probable cause that the vehicle contains contraband; aerial surveillance from 1000 feet (although respondents felt that an aerial search from a lower altitude violated a privacy interest); searches of purses or backpacks of students; and searches of trash bags left on the curb).

162. *Id.* at 364–65.

163. *Id.* at 366. When the question was changed to involve recording an individual's cell phone conversation, 91.7% of respondents agreed that a warrant should be required, compared to 7.1% of respondents who disagreed. *Id.*

164. *Id.* at 366–67.

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

166. Fradella et al., *supra* note 98, at 366–67 (stating that only 7.1% agreed with the Court that electronic monitoring of a vehicle did not constitute a Fourth Amendment search). *See also* McAllister, *supra* note 158, at 515–16 (describing a survey that asked respondents whether a particular type of government surveillance should require a warrant in which 53% of respondents (118 out of 223 who answered the question) believed that police should be required to obtain a warrant before attaching a GPS device to the vehicle of a suspected drug dealer and tracking it for any period of time. However, 23% (51/223) would only require a warrant after ten days of tracking, and 21% (46/223) would allow warrantless tracking for longer than twenty-one days. When the question was changed to involve the tracking of an "innocent suspect," an individual who had not been convicted of any crime and who was

respondents disagreed with the Court's holding that individuals had no reasonable expectation of privacy in bank records.[167]

The accuracy of this study in reflecting societal expectations of privacy may be supported by its relative correspondence with the results of the Intrusiveness Rating Scale developed by Christopher Slobogin in 1993[168] and updated by Jeremy A. Blumenthal in 2009.[169] Out of fifty search-and-seizure scenarios tested in both studies, government monitoring of a telephone conversation was ranked as one of the top ten most intrusive scenarios, justifying the *Katz* decision requiring a warrant before such monitoring can occur.[170] Likewise, respondents ranked "perusing bank records" as a highly-invasive search, corresponding to the finding in the Fradella study that most individuals expressed an expectation of privacy in those records.[171]

not currently suspected of any crime, 89% (205/230) believed that police should be required to obtain a warrant). This survey generally supports the findings of the Fradella study, and provides a more nuanced insight into the privacy expectations concerning GPS tracking of individuals.

167. Fradella et al., *supra* note 98, at 366 (noting that 85.4% felt that individuals retained a privacy interest in bank records, while 5.5% agreed that records may be obtained without a warrant).

168. Slobogin, *supra* note 155, at 730–38. Slobogin has conducted other empirical studies of invasiveness using a similar format to his first study but without the same methodological rigor. *See* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 110–13 (2007).

169. Blumenthal, *supra* note 158.

170. *Id.* at 355 (showing that wiretapping was ranked seventh); Slobogin, *supra* note 155, at 730–38 (ranking wiretapping as second).

171. Slobogin, *supra* note 155, at 730–38 (noting that government search of bank records was ranked the thirteenth most invasive search in the Slobogin study, and the second most invasive in the Blumenthal study). Another point of concurrence between the studies was in "flying 400 yards over backyard in helicopter" and "stopping drivers at roadblock to view occupants"; both consistently ranked as minimally invasive searches in the Slobogin and Blumenthal studies. *Id.* This roughly corresponds to the evidence from Fradella that respondents to that study do not have a strong expectation of privacy in those situations. Fradella et al., *supra* note 98, at 363, 365. But some appreciable variations do exist between the privacy expectation expressed in Fradella and the invasiveness of search in the Slobogin and Blumenthal studies. Whereas an overwhelming majority of respondents to the Fradella study expressed an expectation of privacy in their movements on public roads, "using a beeper to track car" was ranked as relatively non-invasive in the original Slobogin study, and only moderately invasive in the Blumenthal update. Slobogin, *supra* note 155, at 110–13; Blumenthal, *supra* note 158, at 355. Tracking ranked thirty-third in the original study, and seventeenth in the updated study. Moreover, at least one hypothetical situation does not correlate across the three studies. 62.5% of respondents to the Fradella study believed that school officials should be able to search the lockers of students, and did not express a strong expectation of privacy in searches of backpacks or purses of high school students. Fradella et al., *supra* note 98, at 365–66. In the Slobogin and Blumenthal studies, "searching a 6th grader's locker" and "searching high school kid's purse" were ranked as invasive searches, with searching a purse ranked in the top ten most invasive searches. Blumenthal, *supra* note 158, at 358.

The empirical evidence presented in the Fradella study suggests that society's expectations of privacy may be relatively uniform across demographics, and the broad correlation with the invasiveness studies of Slobogin and Blumenthal suggests that those expectations of privacy are relatively stable over time. But the fact that judges are members of society, and are therefore arguably qualified to determine what privacy expectations are accepted by society as reasonable, is an insufficient basis from which to argue that judge-made common law may be a repository of information about societal privacy expectations. The decisions with which the Fradella respondents concurred were those in which the Court found a privacy interest. Rather than showing that the Court accurately assesses societal privacy expectations in all cases, the studies may only suggest that the Court correctly assesses societal expectations when it upholds a reasonable expectation of privacy in some action and does not accurately reflect societal expectations when it rejects a privacy interest. Given this indeterminacy, and recognizing the Court's "hostility to empirical research in the context of adjudicating constitutional claims relevant to criminal law and procedure," it seems clear that privacy interests inherent in the common law are not a robust source of societal privacy expectations.[172]

Notwithstanding all the conceptual problems with the *Katz* test, there is little doubt it will remain the framework for assessing Fourth Amendment privacy rights.[173] Yet the test may be rehabilitated if the Court were to more clearly define the kind of evidence it uses in determining the societal acceptance of privacy expectations. Common law privacy principles like those used by Justice Scalia in *Kyllo* and *Jones* do not seem to be an accurate proxy for societal privacy expectations. Alternatively, the Court may look to state and federal legislation as a source of information concerning the privacy expectations society accepts as reasonable. The following Section shall illustrate why the latter solution is preferable.

172. Fradella et al., *supra* note 98, at 373.

173. *See generally* United States v. Jones, 132 S. Ct. 945 (2012) (Sotomayor, J., concurring) (illustrating that only one current Justice proposes a reevaluation of *Katz* and a related reconsideration of the foundational principles of the Court's Fourth Amendment jurisprudence).

IV. THE NINTH LIFE OF *KATZ*: USING LEGISLATIVE EVIDENCE TO RESOLVE THE EVIDENTIARY GAP IN THE *KATZ* ANALYSIS

A. LEGISLATIVE FACTS AS JUDICIAL EVIDENCE

If common law privacy expectations are not a useful guide for the Court's Fourth Amendment analyses, legislative evidence seems to be an alternative evidentiary source for determining societal expectations of privacy.[174] The *Katz* test expressly declares that the Court will take notice of societal expectations of privacy, expectations that may be illustrated through state and federal legislation.[175] Moreover, Justice Alito's concurrence in *Jones* emphasizes the role of the legislature in addressing the privacy concerns posed by "dramatic technological change."[176]

Legislative evidence not only provides the judiciary with evidence of societal values derived through democratic processes, but Justice Alito at least seems to suggest that legislation may be more responsive to the privacy implications posed by developing technologies than is the Court. In addition, because searches and seizures are increasingly governed by statute,[177] the Court ought to have a quantity of data from which to determine the scope and development of society's expectations of privacy. Yet, the Court tends to disregard state legislation when discussing social expectations of privacy, even though state legislation may be a more timely and more accurate representation of these expectations.[178]

174. Neil Coleman McCabe, *Legislative Facts As Evidence in State Constitutional Search Analysis*, 65 TEMP. L. REV. 1229, 1231 (1992) ("The Supreme Court frequently has relied on legislative or social facts, and its use of such facts has not been confined to Fourth Amendment cases.").

175. Fradella et al., *supra* note 98, at 293 (noting that it may not matter that the judiciary is "a nonmajoritarian institution [and is not] expected to express or implement the will of the people [because] its legitimacy rests on notions of honesty and fairness and, most importantly, on popular perceptions of the judicial decision-making process"). However, acknowledging democratic sources of evidence regarding societal expectations of privacy can only enhance the public's perception of the Court, particularly when the Court's analysis of the Fourth Amendment "explicitly rests on such societal judgments." *Id*.

176. *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.").

177. Kerr, *supra* note 31, at 807.

178. This is true at least when appellants are advocating for recognition of a privacy right. *See* McCabe, *supra* note 174, at 1232–33 ("[T]he Court has rebuffed attempts by claimants to cite in support of the objective reasonableness of Fourth Amendment claims state authority in the form of common law, state constitutions, statutes, or local ordinances. At the same time, the Court has permitted the government to rely on federal and state statutes and regulations in proving that a claimant's expectation of privacy is diminished or unreasonable."). *See also* New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) ("It is one of the happy incidents of the federal system

1. Judicial Deference to State and Federal Legislation

When the Court has taken notice of legislative or social facts, it has largely focused on federal legislation, not state laws. Recall that, with regards to wiretapping, the Court has treated state regulations quite differently, in one case holding that state statutes bore no impact on the Court's constitutional analysis[179] and in another using the statute as a way to illustrate constitutionally deficient legislation for Congress.[180] The Court later articulated its view of the constitutional significance of state law:

> Individual States may surely construe their own constitutions as imposing more stringent restraints on police conduct than does the Federal Constitution. We have never intimated, however, that whether or not a search is reasonable within the meaning of the Fourth Amendment depends on the law of the particular State in which the search occurs.[181]

Although state laws may not control constitutional interpretation, the Court does recognize that state legislation conveys information about societal values—information that the Court may integrate into its subsequent constitutional interpretation.[182]

While the Court has been inconsistent in its treatment of state laws, it has shown deference to "comprehensive" federal legislation.[183] Once Congress enacted the Wiretap Act, courts declined to consider constitutional challenges to wiretapping, recognizing that Congress instituted a statutory framework to balance the privacy interests of individuals against the needs of law enforcement.[184]

---

that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.").

179. *See* Olmstead v. United States, 277 U.S. 438, 469 (1928).

180. *See* Berger v. New York, 388 U.S. 41, 63–64 (1967).

181. California v. Greenwood, 486 U.S. 35, 43 (1988) (italics in original, internal citations omitted). The Court stated further that "Fourth Amendment analysis must turn on such factors as 'our societal understanding that certain areas deserve the most scrupulous protection from government invasion.'" *Id.*

182. Dru Stevenson, *Judicial Deference to Legislatures in Constitutional Analysis*, 90 N.C. L. REV. 2083, 2126 (2012).

183. *See* United States v. Jones, 132 S. Ct., 945 964 (2012) (Alito, J., concurring) ("Congress did not leave it to the courts to develop a body of case law governing [wiretapping]. . . . Instead, Congress promptly enacted a comprehensive statute and since that time, the regulation of wiretapping has been governed primarily by statute and not by case law."); Kerr, *supra* note 31.

184. *See supra* Section II.C.

All this suggests that the Court would look to federal privacy legislation, and not state statutes, to provide some indication of the privacy interests that society accepts as reasonable. However, while the regulatory structure established by the Wiretap Act has continued to control government telephone surveillance, Congress has largely failed to update the other statutes controlling electronic surveillance to reflect technological developments, making federal legislation less indicative of societal expectations.[185]

2. Federal Legislation Does Not Reflect Accepted Societal Privacy Expectations

Since the Wiretap Act was passed in 1968, Congress has passed three statutes that significantly supplemented or amended the Wiretap Act: the Foreign Intelligence Surveillance Act (1978)[186] ("FISA"), the Electronic Communications Privacy Act (1986)[187] ("ECPA"), and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (2001)[188] ("USA-PATRIOT"). FISA regulates surveillance for national security or foreign intelligence purposes.[189] ECPA comprehensively restructured the Wiretap Act, combining the Wiretap Act, the Stored Communications Act, and the Pen Register Act into a single legislative system. Finally, USA-PATRIOT made modifications to both FISA and ECPA, altering those regulatory schemes to "update, strengthen, and expand laws governing the investigation and prosecution of terrorism."[190]

a. Foreign Intelligence Surveillance Act

Because the Wiretap Act did not regulate surveillance for national security proposes, "presidents claimed a prerogative to conduct national

185. Solove, *Fourth Amendment Codification*, *supra* note 9, at 770–71.

186. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801–1811 (2000)).

187. Electronic Communications Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

188. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107-56, 115 Stat. 272 (codified as amended in scattered sections of 8 U.S.C., 15 U.S.C., 18 U.S.C., 31 U.S.C., 42 U.S.C., 49 U.S.C., 50 U.S.C.).

189. Solove, *Reconstructing Electronic Surveillance Law*, *supra* note 17, at 1266.

190. U.S. DEPARTMENT OF JUSTICE, REPORT FROM THE FIELD: THE USA PATRIOT ACT AT WORK (July 2004).

security wiretapping without judicial approval."[191] Following a congressional investigation into federal abuses of wiretaps, Congress separated domestic and foreign surveillance and regulated the latter through FISA. FISA authorizes foreign electronic surveillance pursuant to court orders, which are reviewed by a secret court consisting of eleven federal district court judges.[192]

Whereas the Wiretap Act defines strict protections for domestic wiretapping,[193] FISA requirements are much looser and weigh in favor of the government.[194] Among other differences with domestic wiretapping, under FISA the government only needs to establish probable cause that the monitored party is a "foreign power" or an "agent of a foreign power," not that there is probable cause that the surveillance would uncover evidence of criminal activity.[195] Moreover, FISA surveillance can continue three times as long as domestic surveillance. Finally, evidence gathered under the permissive FISA standards may be used for domestic criminal prosecution.[196]

The USA-PATRIOT Act expanded the scope of FISA, allowing government surveillance under the more forgiving standard so long as foreign intelligence gathering is "a significant purpose" of the investigation.[197] Following this change, a FISA application by the government would only be denied if the "government's sole objective is merely to gain evidence of past criminal conduct," and granted in all other cases.[198] Although the FISA Amendments Act of 2008[199] imposed a requirement that the government to obtain a warrant when the target of FISA surveillance is within the United States or is a U.S. citizen, U.S.

191. SCHULHOFER, *supra* note 25, at 156. *See also* Solove, *Reconstructing Electronic Surveillance Law*, *supra* note 17, at 1276 ("[E]very president from Franklin D. Roosevelt to Richard M. Nixon improperly used government surveillance to obtain information about critics and political opponents.").

192. Solove, *Reconstructing Electronic Surveillance Law*, *supra* note 17, at 1289.

193. *See supra* text accompanying notes 70–71.

194. Solove, *Reconstructing Electronic Surveillance Law*, *supra* note 17, at 1290. Because government applications for FISA surveillance are argued ex parte and may be appealed following an adverse ruling, "the government thus gets two bites at the apple, and the courts only hear the government's side." *Id.*

195. *Id.*

196. *Id.*

197. *Id*. at 1290–91.

198. *Id*. at 1291.

199. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110–261, 122 Stat 2436 (codified as amended in scattered sections of 8 U.S.C., 47 U.S.C., 50 U.S.C.).

citizens may still be the subject of this permissive surveillance so long as they are not the direct target.[200]

The pervasive secrecy surrounding government surveillance under FISA largely insulates it from popular disapproval.[201] Even as the scope of the minimally restrictive searches under FISA expands and leads to surveillance of increasing numbers of American citizens, the level of secrecy surrounding the surveillance prevents the potential subjects of that surveillance from having any certainty that surveillance has occurred.[202] This makes FISA of little evidentiary value in indicating what privacy expectations society accepts as reasonable.

b. Electronic Communications Privacy Act

Twenty years after the passage of the Wiretap Act, Congress became concerned with increasing threats to privacy posed by new technologies and updated and reorganized the Wiretap Act by passing the ECPA.[203] The ECPA governs domestic surveillance and includes three sections: Title I (the Wiretap Act), Title II (the Stored Communications Act), and Title III (the Pen Register Act).[204] However, none of these sections have been substantially amended in subsequent years,[205] and the gaps in the Wiretap Act allow particular types of government surveillance to occur without legislative regulation.[206]

Title I provides relatively strong protections for the content of electronic communications while in transit, requiring a "warrant-like order

200. SCHULHOFER, *supra* note 25, at 158–59.

201. *Id.* at 159 (illustrating that the 2008 amendments show that "political leaders occasionally (if not promptly) can transcend national security panic and unthinking deference" to military and intelligence needs).

202. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2012) (finding that citizens did not have standing to challenge FISA surveillance because they did not have information indicating that they had been the subject of such surveillance).

203. Mulligan, *supra* note 21, at 1557, 1558. The ECPA emerged from a "growing consensus" in Congress that telecommunications and computing advances were outpacing existing privacy protections; at that time, businesses were just beginning to use email, only 5% of households had personal computers, and home internet access was rare. *Id.* at 1560–61.

204. *Id.* at 1565.

205. The USA-PATRIOT Act made a number of changes to the ECPA, but the direct amendments to the ECPA were relatively minor structural changes. Solove, *Reconstructing Electronic Surveillance Law*, *supra* note 17, at 1277–78.

206. For example, Title I governs communications intercepted while in transmission, and defines communications as including "aural transfers"; therefore, it does not regulate silent video recordings, so long as the government does not "intercept" the video surveillance. *Id.* at 1280.

based on probable cause" before the information may be accessed.[207] Weaker protections are provided by Title II for electronic communications stored longer than 180 days by a service provider;[208] access may be provided pursuant to a subpoena, which is granted upon showing "specific and articulable facts showing . . . reasonable grounds [that the] communications are relevant to the criminal investigation."[209] Finally, identifying information of electronic communications, extended by the USA-PATRIOT Act to include email headers, IP addresses, and web-site addresses, may be obtained upon the government certifying that "information likely to be obtained . . . is relevant to an ongoing investigation."[210]

These divisions are not entirely rational, as the same communication may receive different levels of protection depending on whether it is in transit or in storage, whether it has been read or not, and whether the information is communicated orally or in writing.[211] The ECPA reflects an outdated understanding of electronic communication.[212]

Moreover, the wire and oral communications described in Title I are enforced by an exclusionary rule, preventing illegally obtained surveillance from being used in a trial.[213] However, neither Title II nor Title III includes an exclusionary protection, broadly negating the relatively weak protections provided by the legislation.[214] Despite the Court often curtailing

207. Mulligan, *supra* note 21, at 1566. However, only "oral" and "wire" communications, and not emails or other electronic communications, are protected by an exclusionary rule. Solove, *Reconstructing Electronic Surveillance Law*, *supra* note 17, at 1282.

208. For communications stored less than 180 days, a warrant is required. Solove, *Reconstructing Electronic Surveillance Law*, *supra* note 17, at 1284–85.

209. *Id*. at 1284. The definitions of "stored communications" and the scope of the legislation is vastly complicated; in general, all electronic communications, except unopened emails newer than 180 days may be accessed with a subpoena, which may issue on a showing of relevance and without judicial oversight. Mulligan, *supra* note 21, at 1570.

210. Solove, *Reconstructing Electronic Surveillance Law*, *supra* note 17, at 1287–88.

211. For example, the same email may be protected by Title I while being transmitted and protected by Title II while waiting on a third-party server to be downloaded, and the addressing information, including the sender and recipient of the email, is covered by Title III. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY, *supra* note 157, at 168–70.

212. The minimal protections for addressing information is especially troubling, as web site addresses now convey a great amount of information about an individual, and IP addresses can be used to track an individual's movements, just as the FBI did in discovering the movements and activities of Ms. Broadwell. *See* Solove, *Reconstructing Electronic Surveillance Law*, *supra* note 17, at 1287; Zetter, *supra* note 15.

213. Solove, *Reconstructing Electronic Surveillance Law*, *supra* note 17, at 1282, 1283.

214. *Id*. at 1285, 1289.

the application of the legislative exclusionary rules,[215] the presence of an exclusionary rule in Title I suggests that it is "comprehensive" legislation, insofar as it defines significant penalties for government disobedience. Since Title II and Title III do not include a legislative exclusionary rule and instead rely upon the judiciary to administer the penalties for violation of the legislative rules, these statutes may not be the kind of "comprehensive" legislation to which Justice Alito suggested that the Court might defer.[216]

The ECPA does not clearly suggest what privacy expectations society accepts as reasonable because the ECPA has not been updated to reflect the dramatic changes that occurred with regards to electronic communications in the past twenty-eight years, and because it does not seem to be "comprehensive" legislation. As neither judge-made common law nor federal privacy legislation indicates societal expectations, state privacy legislation may be the best resource to determine societal privacy expectations.

3. State Legislation Has Provided Evidence of Societal Privacy Expectations

Traditional democratic theory suggests that majoritarian legislatures are best able to represent societal values, implying that legislation is the best indication of the expectations of privacy held by society.[217] As discussed above, federal legislation concerning electronic surveillance is dated and inadequate, and therefore it does not clearly represent societal values. State legislation may be the best resource to demonstrate societal expectations of privacy.

Although the Court held that the state regulation of wiretapping in *Olmstead* had no bearing on the admissibility of wiretap evidence in federal cases and overturned New York's wiretapping statute in *Berger*, the Court

215. George E. Dix, *Nonconstitutional Exclusionary Rules in Criminal Procedure*, 27 AM. CRIM. L. REV. 53, 69 (1989) ("In interpreting the statutory exclusionary rule in the federal electronic surveillance statute, the Supreme Court has held that despite the unqualified language of the statute Congress did not intend violation of any provision of the scheme to mandate exclusion.").

216. *Cf.* Michael S. Leib, *E-Mail and the Wiretap Laws: Why Congress Should Add Electronic Communication to Title III's Statutory Exclusionary Rule and Expressly Reject A "Good Faith" Exception*, 34 HARV. J. ON LEGIS. 393, 396 (1997) ("In order to procure Department of Justice support and assure passage of the ECPA, Congress agreed not to add electronic communication to the statutory exclusionary rule. . . . [Instead, electronic communication not covered by Title I,] even if illegally intercepted, is subject only to the Fourth Amendment exclusionary rule, whereas wire and oral communication enjoy much broader protection.").

217. Stevenson, *supra* note 182, at 2122.

has accepted state legislation as persuasive authority on a number of occasions.[218] The Court seems to find that societal understandings may be as equally illustrated through state statutes as through federal statutes, so long as sufficient numbers of states have legislated and the legislation therefore represents a national trend.[219]

Yet, it is not clear under what circumstances the Court finds such legislation to be indicative of a national trend and when it does not. At times the Court finds that state legislation is persuasive only when a numerical majority of states have enacted similar legislation,[220] and at other times the Court recognizes a "developing trend" among states, even when the states with progressive legislation are a small minority.[221] Moreover, the Court seems more likely to accept the existence of state legislation as evidence to refute privacy expectations, not to establish privacy rights. For example, warrantless searches of "pervasively regulated businesses" and automobiles were held constitutional because state legislation has made the public "fully aware" that it has a reduced expectation of privacy.[222] Alternatively, when state laws have granted privacy rights, the Court has understood those laws not to indicate the understanding of "society as a whole," but merely a "concept[] of privacy under the laws of each state."[223]

218. *Id.* at 2125. As an example, the Court has held that the Eighth Amendment's prohibition of cruel and unusual punishments should be interpreted in light of "the evolving standards of decency that mark the progress of a maturing society." Trop v. Dulles, 356 U.S. 86, 101 (1958). The Court subsequently held that "the clearest and most reliable objective evidence of contemporary vales is the legislation enacted by the country's legislatures" and that "first among the objective indicia that reflect the public attitude towards a given sanction are statutes passed by society's elected representatives." Stevenson, *supra* note 182, at 2127.

219. McCabe, *supra* note 174, at 1251–52.

220. *Compare* Bowers v. Hardwick, 478 U.S. 186, 192–94 (1986) ("When the Fourteenth Amendment was ratified, all but 5 of the 37 States in the Union had criminal sodomy laws. In fact, until 1961, all 50 States outlawed sodomy, and today, 24 States and the District of Columbia continue to provide criminal penalties for sodomy performed in private and between consenting adults."), *with* Lawrence v. Texas, 539 U.S. 558, 573 (2003) ("The 25 States with laws prohibiting the conduct referenced in *Bowers* are reduced now to 13, of which 4 enforce their laws only against homosexual conduct.").

221. Stevenson, *supra* note 182, at 2108. *Cf.* Mapp v. Ohio, 367 U.S. 643, 651–52 (1961) ("[I]n 1949, . . . almost two-thirds of the States were opposed to the use of the exclusionary rule, now . . . more than half of those . . . by their own legislative or judicial decision, have wholly or partly adopted or adhered to the [the exclusionary] rule. Significantly, among those now following the rule is California . . . .") (internal citations omitted).

222. McCabe, *supra* note 174, at 1236–37.

223. California v. Greenwood, 486 U.S. 35, 44 (1988). *See generally* Berger v. New York, 388 U.S. 41 (1967) (overturning representative state wiretap laws).

Thus, the Court appears to find legislative or social facts to be persuasive evidence of societal understanding when those facts bolster its conclusion or support its argument; but when state legislation conflicts with the Court's interpretation, the legislation is either in conflict with "developing trends" or does not represent the understanding of "society as a whole."[224] This inconsistency adds to the confusion and indeterminacy of the Court's Fourth Amendment jurisprudence. It suggests that the Court's decisions are based on judicial presumptions and preconceptions rather than the nominally objective evidence of societal expectations of privacy, as suggested by state legislation.[225]

V. CONCLUSION

The Wiretap Act has endured as the preeminent example of search-and-seizure legislation, striking an appropriate balance between the legitimate needs of law enforcement while protecting an individual's expectation of privacy. However, the Wiretap Act emerged because Congress was unable to pass adequate legislation for the previous thirty-three years, requiring states to fill the gap left by Congress' inaction. Although the Court overturned New York's legislation in *Berger*, it highlighted the constitutional defects and encouraged Congress to enact comprehensive legislation that avoided these defects.

Now, the ECPA is a similarly incomplete and imbalanced legislation governing electronic surveillance, and Congress has entirely failed to regulate certain recent technological developments. Yet, few states have passed supplementary legislation to the ECPA; the Court is therefore unlikely to find that the state legislation that has been enacted illustrates the understanding of "society as a whole," which leaves the Court unable to refer to alternative legislative schemes when adjudicating challenges to the federal laws.[226] The Court must thereby determine the scope of societal

224. McCabe, *supra* note 174, at 1231.

225. *See* Fradella et al., *supra* note 98, at 293–94.

226. For example, the state response to the Court's decision in *Jones* has been largely judicial, not legislative. *See generally* Marjorie A. Shields, Annotation, *Fourth Amendment Protections, and Equivalent State Constitutional Protections, as Applied to the Use of GPS Technology, Transponder, or the Like, to Monitor Location and Movement of Motor Vehicle, Aircraft, or Watercraft*, 5 A.L.R. 6th 385 (2008). Moreover, a number of states do have prohibitions on vehicle tracking by private individuals, but the extent and character of that prohibition varies widely. *See* SMITH, PRIVACY JOURNAL'S COMPILATION OF STATE AND FEDERAL PRIVACY LAWS, *supra* note 73 (describing state vehicle tracking laws).

expectations of privacy without any legislative evidence and has resorted to mining the common law for evidence of enduring, universal societal expectations.

The Court's recourse to the common law may allow it to resolve individual cases without having to determine the impact of new technologies on the alleged privacy interest,[227] but the Court risks misinterpreting the impact of technological development. Two solutions to the Court's "contentious jurisprudence" are proposed below.[228]

A. ABANDON THE *KATZ* TEST

The *Katz* test has the supposed advantage of providing a fluid standard that may be easily applied to new technological innovations. But the test has not provided the expected flexibility and instead has required the Court to engage in an unsuitable analysis of societal expectations of privacy. The Court is rightfully wary of considering empirical data concerning societal expectations of privacy, and both state and federal legislatures have been largely unable to respond to new forms of electronic surveillance. Moreover, although new surveillance technologies may be superficially similar to preceding technologies, modern technology can produce a detailed and broad picture of an individual, entailing a very different violation of privacy than did the earlier technology.[229]

Given the criticism of the *Katz* test and the Court's difficulties in assessing societal expectations, the Court should return to its strengths and assess Fourth Amendment claims using a reasonableness standard. The Court's interpretation of Justice Harlan's concurrence in *Katz* has not led to strong or consistent privacy protections,[230] and has produced a haphazard jurisprudence. However, another paragraph in Justice Harlan's concurrence suggests that the Court ought to focus on the reasonableness of a Fourth Amendment search, not on whether the search meets the two-prong test he articulated: he writes that "the invasion of a constitutionally protected area by federal authorities is . . . presumptively unreasonable in the absence of a

227. *See* City of Ontario v. Quon, 130 S. Ct. 2619, 2635 (2010) (Scalia, J., concurring) ("Applying the Fourth Amendment to new technologies may sometimes be difficult, but when it is necessary to decide a case we have no choice.").

228. Solove, *Fourth Amendment Pragmatism*, *supra* note 7, at 1511.

229. *See generally* United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) (discussing that GPS surveillance allows the government to compile a "precise, comprehensive record of a person's public movements"); McAllister, *supra* note 158.

230. Solove, *Reconstructing Electronic Surveillance Law*, *supra* note 17, at 1302–03.

search warrant."[231] By adhering to this presumption, the Court would be better able to create a consistent standard for Fourth Amendment searches, one which accounts for the "more sophisticated [surveillance] systems" that will inevitably arise.[232]

B. LEGISLATURES SHOULD LEGISLATE

State and federal legislation has failed to keep pace with technological innovation; moreover, recent technological developments present unique challenges to existing categories, making analogical reasoning to previous technology a flawed and inadequate response.[233] While federal legislation covering electronic surveillance is particularly out of date, having been last updated by the USA-PATRIOT Act in 2001, state legislatures have not consistently addressed the newly developed surveillance technologies either. Although many bills concerning new threats to privacy have been proposed, few have been passed.[234]

However, California Governor Brown's suggestion that "courts are better suited to resolve the complex and case-specific issues relating to constitutional search-and-seizures protections"[235] is not the solution. Given that the *Katz* test is likely to continue to control the Court's analysis and the evidentiary problems with the test are likely to remain, federal and state legislatures should be encouraged to pass legislation controlling electronic surveillance. Legislatures can enact "comprehensive rules far ahead of current practice," as Congress did in passing the ECPA.[236]

To encourage such legislation, the Court should be transparent about which evidence it accepts as demonstrating societal expectations of privacy. If the Court accepts that legislative facts are the most democratic and reasonable source of evidence of societal expectations, it should

231. *See* Katz v. United States, 389 U.S. 347, 361–62 (1967) (Harlan, J., concurring).

232. Kyllo v. United States, 533 U.S. 27, 36 (2001).

233. McAllister, *supra* note 158, at 477.

234. *See* Allie Bohm, Status of Domestic Drone Legislation in the States, AM. CIV. LIBERTIES UNION (February 15, 2013, 12:21 PM), https://www.aclu.org/blog/technology-and-liberty/status-domestic-drone-legislation-states (describing that thirty states have proposed legislation regulating government use of domestic drones, but few have enacted the legislation).

235. Amy Gahran, *California Governor Allows Warrantless Search of Cell Phones*, CNN (October 11, 2011 12:31 PM), http://www.cnn.com/2011/10/11/tech/mobile/california-phone-search-veto/index.html.

236. Kerr, *supra* note 31, at 870. *See also* Mulligan, *supra* note 21, at 1565 ("[T]he ECPA was both a proactive and a reactive statute . . . [because it was] an effort to head off the possibility of courts concluding that the Fourth Amendment did not protect electronic communications . . . .").

encourage states and Congress to create rules governing emerging methods of electronic surveillance by indicating that such legislation would be assessed deferentially and be taken into account in the continuing development of Fourth Amendment jurisprudence. This does not mean that the Court should defer to the legislature, or that legislation is inherently protective of privacy rights.[237] Rather, if the Court is committed to a Fourth Amendment analysis that reflects the expectations of privacy society accepts as reasonable, it must have a basis for making that determination. Embracing state and federal privacy legislation as indicative of society's expectations of privacy is the best way for the Court to develop a consistent and coherent Fourth Amendment analysis.

237. *See* Hanni Fakhoury, *EFF Again Reminds Court Forced Warrantless DNA Collection Violates Fourth Amendment*, ELEC. FRONTIER FOUND. (Mar. 20, 2012), https://www.eff.org/deeplinks/2012/03/eff-again-reminds-court-forced-warrantless-dna-collection-violates-fourth ("[T]he federal government and 47 states [are] collecting DNA from convicted felons, and 22 states and the federal government [are] collecting DNA from individuals merely arrested for a crime.").