The Heritage Foundation
LEADERSHIP FOR AMERICA

LEGAL MEMORANDUM

No. 102 | SEPTEMBER 19, 2013

The Fourth Amendment and New Technologies

Paul J. Larkin, Jr.

Abstract

The Fourth Amendment was not designed to serve as a static protection against government abuse. No provision of the Bill of Rights—particularly one outlawing "unreasonable" searches and seizures—could or should be cabined to the specific historical incidents that gave it birth. That construction would render the amendment a safeguard for the peculiar historical incidents that troubled late eighteenth century Americans rather than a guarantee that law enforcement officers act reasonably today and tomorrow. At the same time, the Framers would not have found unimaginable the need to make a trade-off between liberty and security, or to reassess that trade-off as times change. How will the Supreme Court make that trade-off with regard to technologies unheard of two decades ago, to say nothing of two centuries ago?

Law is the formal embodiment of rules that legislators, regulators, and judges etch into statute books, administrative manuals, and judicial decisions. It is unavoidable and desirable to see the law change as technology becomes increasingly sophisticated.

Before there were automobiles and aircraft, there was no need for a law prohibiting their theft.[1] Similarly, before there were telecommunications systems, there was no need for a law to protect the integrity of the conversations of subscribers.[2] And before there were electronic devices such as satellites, digital cameras, and Cray computers, there was no reason to be concerned with the government's use of those tools to find, identify, acquire, analyze, and store significant amounts of information about Americans.

This paper, in its entirety, can be found at **http://report.heritage.org/lm102**

Produced by the Edwin Meese III Center for Legal and Judicial Studies

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Key Points

- It is unavoidable and desirable to see the law change as technology becomes increasingly sophisticated.
- New technologies are a reality and society must decide how to regulate their use—particularly with regard to government surveillance.
- The use of those devices for law enforcement offers potential benefits and costs, and society ought to debate the pros and cons of the trade-off between efficiency and efficacy of law enforcement techniques and the privacy rights of citizens the government may wish to monitor.
- Predicting where the Supreme Court will take Fourth Amendment law in connection with new technologies based on the few and vague suggestions set forth in the majority, concurring, and dissenting opinions in cases such as *Kyllo, Jones, Jardines*, and *King* is a hazardous undertaking

Today, however, these new technologies are a reality and society must decide how to regulate their use—particularly with regard to government surveillance. The use of those devices for law enforcement offers potential benefits and costs, and society ought to debate the pros and cons of the trade-off between efficiency and efficacy of law enforcement techniques and the privacy rights of citizens the government may wish to monitor.

The opportunity for such a debate arises because of the public nature of criminal trials and the constitutional evidentiary rules governing the government's use of evidence acquired by modern surveillance technology. If the government seeks to prove a defendant's guilt by using evidence derived from its reliance on advanced technologies, defendants can demand that the courts review the legality of the government's conduct, and judges will be forced to bless or condemn the use of whatever evidence the government seeks to introduce. Those decisions then define what the Fourth Amendment means.

The Relationship Between the Fourth Amendment and Technology

The Fourth Amendment provides as follows:

> 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.

The amendment prohibits the government from conducting unreasonable "searches" and "seizures." The exclusionary rule enforces the amendment by prohibiting federal, state, or local judges from admitting in the government's case-in-chief evidence obtained in violation of the Fourth Amendment.[3] Parties injured by an unlawful search or seizure can also bring a damages action against the officers involved, but the exclusionary rule has made criminal trials the most likely forum for a public airing of competing versions of what the Fourth Amendment should protect.

Yet, even though the Fourth Amendment has been a fundamental part of American jurisprudence for nearly 225 years—and the exclusionary rule a constitutionally required remedy for nearly a century[4]—the question of whether reliance on sensory-enhancing technology can render a search or seizure unreasonable is a relatively new one. No one seems to have challenged a sheriff's use of spectacles or torches to improve his day or night vision,[5] although it is certain that one or more constables or local residents called out as part of a "hue and cry" or Old West posse must have used them. Perhaps, glasses and torches were so widely used and seemed so reasonable that no one thought to question them, or perhaps they were used, not to acquire proof of a suspect's guilt, but just to find him. Whatever the reason, it seems that it was not until society harnessed electricity and invented telephones that anyone thought to challenge law enforcement's use of sensory-enhancement technology.

The Supreme Court first addressed the issue in 1927. Specifically, in *United States v. Lee,*[6] the Court held that shining a deck-mounted spotlight onto the open deck of a vessel used for rum running did

1. *See* McBoyle v. United States, 283 U.S. 25 (1931) (ruling that "aircraft" were not "vehicles" under the federal law prohibiting the theft of the latter).
2. *See* Katz v. United States, 389 U.S. 347 (1967) (ruling that interception of a person's conversations made over a public pay phone is a "search" for Fourth Amendment purposes).
3. Professor Wayne LaFave's multi-volume treatise on the Fourth Amendment is the best in-depth discussion of the development of the case law defining its terms and the remedies for violations. *See* 1–6 Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment (4th ed. 2004).
4. The Supreme Court created the exclusionary rule in Weeks v. United States, 242 U.S. 383 (1914), as a remedy for Fourth Amendment violations committed by the federal government. The Court required that state courts apply the rule as a remedy for violations by their own state and local police officers in Mapp v. Ohio, 367 U.S. 643 (1961).
5. Unaided observation could not constitute a "search." *See* Boyd v. United States, 116 U.S. 616, 628 (1886) ("'[T]he eye cannot by the laws of England be guilty of a trespass.'") (quoting Entick v. Carrington, 19 How. St. Tr. 1029, 95 Eng. Rep. 807 (K.B. 1765)).
6. 274 U.S. 559 (1927).

not constitute a "search" for purposes of the Fourth Amendment.[7] Rather than treat the defendant's claim as raising a novel Fourth Amendment issue, the Court gave it the back of the hand.[8]

The following year, the Court held in *Olmstead v. United States*[9] that the interception of telephone communications not requiring a physical trespass onto a person's property—colloquially known as "bugging"—also did not constitute a search or seizure. The officers listened in on Olmstead's phone conversation, not by entering his home, but by attaching intercept equipment to phone lines found elsewhere. Because that form of eavesdropping did not involve a trespass, the Court ruled that a search had not occurred.

That is where the law stood for the next four decades,[10] until 1967, when the Supreme Court decided *Katz v. United States*.[11]

The issues raised in *Katz* stem from the following fact pattern: Charles Katz was using a public outdoor telephone booth to engage in an activity familiar to all March Madness fans: gambling on sporting events. Unbeknownst to Katz, the FBI had attached an electronic listening and recording device to the outside of the phone booth, and the government used the content of his recorded communications against Katz at a trial for violating the federal gambling laws. Breaking new ground, the Supreme Court reversed, ruling that the government had unlawfully violated Katz's privacy interest in the content of his conversations.

The Court started by noting that "the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase 'constitutionally protected area'" and that "the Fourth Amendment cannot be translated into a general constitutional 'right to privacy.'"[12] As the Court reasoned, the Fourth Amendment "protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all."[13]

Eschewing its prior use of the term "constitutionally protected area" to define the scope of the Fourth Amendment,[14] the Court wrote that asking whether an outdoor public phone booth was "a constitutionally protected area" was a mistake,[15] because "the Fourth Amendment protects people, not places."[16] On the one hand, the Court reasoned, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection," while, on the other hand, "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[17]

The fact that Katz was visible when he used the telephone was irrelevant, the Court noted, because what Katz could justifiably seek protection from was

7. *Id.* at 563.

8. The Court's entire discussion of the issue was the following: "[N]o search on the high seas is shown. The testimony of the boatswain shows that he used a searchlight. It is not shown that there was any exploration below decks or under hatches. For aught that appears, the cases of liquor were on deck and, like the defendants, were discovered before the motorboat was boarded. Such use of a searchlight is comparable to the use of a marine glass or a field glass. It is not prohibited by the Constitution." *Id.*

9. 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

10. *See, e.g.*, Lee v. United States, 343 U.S. 747 (1952) (use of a microphone and "body wire" on an agent to record a conversation is not a "search"); Goldman v. United States, 316 U.S. 129, 135–36 (1942) (use of a "detectaphone," a device that, when placed on the outside of an adjoining wall, could transmit sound waves into voice communications, was not a "search"). The Supreme Court's decision in Silverman v. United States, 365 U.S. 505 (1961), raised hope that the Court might change the course it first set in *Olmstead*. In *Silverman* the Court held unlawful the use of a "spike mike," a microphone inserted into a private residence that, when it touched a metal heating duct, transformed the entire heating system into a giant microphone. But *Silverman* involved a physical intrusion into a home, the most protected of the structures covered by the Fourth Amendment, so it was uncertain whether *Silverman* signaled a change in direction or was just a way station along a well-trodden route.

11. 389 U.S. 347 (1967).

12. 389 U.S. at 350.

13. *Id.*

14. *See, e.g.*, Hoffa v. United States, 385 U.S. 293, 301-02 (1966); Silverman v. United States, 365 U.S. 505, 510 (1961).

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

16. *Id.*

17. *Id.*

not "the intruding eye," but "the uninvited ear."[18] Concluding that "searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment subject only to a few specifically established and well-delineated exceptions,"[19] none of which was applicable there, the Court ruled that the government's conduct violated the Fourth Amendment.

Katz seemed to be a watershed decision in Fourth Amendment law. The Court rejected the proposition that common law trespass law defined the scope of the Fourth Amendment[20] and appeared to endorse the two-pronged test, articulated by Justice Harlan in his concurring opinion: the Fourth Amendment safeguards privacy interests that an individual and society deem reasonable.[21] *Katz* signaled that the Supreme Court might rethink its entire approach to Fourth Amendment coverage by using privacy rather than property concepts. Some applauded that prospect; others feared it. As it turned out, however, the Court did not go very far down the road that supporters and critics anticipated.

Post-*Katz* Case Law

The Court often has reiterated the two-pronged inquiry that Justice Harlan articulated in *Katz* as a means of defining a "search."[22] At the same time, however, the Court has not eschewed reliance on property rules to define the contours of searches and seizures, and, on occasion, has specifically relied on such rules in determining whether a search or seizure has occurred. For example, the Court in *Katz* ruled that a person who enters a phone booth does not assume the risk of being overheard. By contrast, in *United States v. White,*[23] the Court held that a person who invites someone into his or her home assumes the risk, not only of being betrayed, but also of being recorded. *Katz* rejected reliance on arcane rules of property law to define the scope of the Fourth Amendment. By contrast, *Oliver v. United States*[24] reaffirmed the proposition that the Fourth Amendment does not apply to the "open fields" because the crown could enter upon them at common law.[25] The Court in *Katz* endorsed a privacy-based approach to the Fourth Amendment. By contrast, the Court in *United States v. Miller*[26] and *Smith v. Maryland*[27] concluded that once a person allows someone else access to personal information, any privacy interest in that information is gone forever.[28] And recently in *United States v. Jones,*[29] the Court held that the physical placement of a GPS tracking device on a person's vehicle and subsequent

18. *Id.* at 352.

19. *Id.* at 357.

20. *Id.* at 352–53.

21. *Id.* at 361 (Harlan, J., concurring) ("As the Court's opinion states, 'the Fourth Amendment protects people, not places.' The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a 'place.' My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.").

22. *See, e.g.*, Maryland v. King, 133 S. Ct. 1958, 1978 (2013); Skinner v. Ry. Labor Executives Ass'n, 489 U.S. 602, 617 (1989); Rakas v. Illinois, 439 U.S. 128, 143 (1979).

23. 401 U.S. 745 (1971).

24. 466 U.S. 170 (1984); *see also* United States v. Dunn, 480 U.S. 294 (1987).

25. *See* Hester v. United States, 265 U.S. 57, 59 (1924) ("The only shadow of a ground for bringing up the case is drawn from the hypothesis that the examination of the vessels took place upon Hester's father's land. As to that, it is enough to say that, apart from the justification, the special protection accorded by the Fourth Amendment to the people in their 'persons, houses, papers and effects,' is not extended to the open fields. The distinction between the latter and the house is as old as the common law.") (citing 4 Blackstone, Commentaries *223, 225-26).

26. 425 U.S. 435 (1976) (bank records).

27. 442 U.S. 735 (1979) (telephone number dialed).

28. *Cf.* SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984) ("It is established that, when a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities.").

29. 132 S. Ct. 945 (2012).

monitoring of its movements constituted a search for Fourth Amendment purposes, because the placement constituted a trespass under the common law.

As a result of these decisions, parties who had hoped for a revolution in Fourth Amendment law have been disappointed—not only by the results of the Supreme Court's post-*Katz* case law, but also by what they see as the Court's abandonment of its promised concern for individual privacy. As Professor Anthony Amsterdam once wrote: "I can conceive of no rational system of concerns and values that restricts the government's power to rifle my drawers or tap my telephone but not its power to infiltrate my home or my life with a legion of spies."[30]

For privacy advocates, however, all is not lost. In recent Supreme Court case law there have been stirrings of a renewed interest in a privacy-based analysis of the Fourth Amendment. A few decisions have given privacy advocates hope that perhaps the Court is concerned after all about the use of new technologies to intrude on Americans' "persons, houses, places, and effects." For example, in *Kyllo v. United States,*[31] the Court held that use of thermal-imaging technology—a device that measures heat emissions from within a structure—to learn what is transpiring within a home did, in fact, constitute a search. Similarly, in *Florida v. Jardines,*[32] the Court found that a new use for an old technology—i.e., a dog's exceptional ability to sniff out items such as drugs—can amount to an invasion of privacy if the dog is in a place that man's best friend is not entitled to be.[33] And, in *Maryland v. King,*[34] a closely divided Court upheld the use of suspicionless buccal swabbing (a relatively non-invasive way of collecting cells from the inside of one's cheek) for the purpose of performing a DNA analysis of an arrestee only in limited circumstances (i.e., the arrest was for a serious crime, and the DNA analysis did not disclose genetic or medical information) and so long as the information gleaned was not recorded in a database compiling genetic or medical information.[35] Indeed, privacy advocates are particularly encouraged by the fact that the Court's newfound interest in privacy protection seems to extend across the conservative-liberal divide[36]

How Will the Supreme Court Apply the Fourth Amendment to New Technologies?

The *Kyllo, Jones, and King* cases offer excellent examples of technologies that did not exist when the Supreme Court decided *Katz*. And there are a host of other information gathering, analyzing, and recording devices that raise the same types of concerns that motivated the Court in *Katz* to focus on a person's privacy—rather than property rights—as the locus of Fourth Amendment concern.

Consider the Global Positioning Satellite (GPS) system.[37] The GPS system identifies a specific person's cell phone location within meters.[38] Cell phone manufacturers and telecommunications companies

30. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 Minn. L. Rev. 349, 365 (1974).

31. 533 U.S. 27 (2001).

32. 133 S. Ct. 1409 (2013).

33. In *Jardines* a police officer took his drug-sniffing dog "Franky" onto the porch of a private home, an area within the curtilage surrounding a home that is entitled to be treated as the home itself, without either a search warrant or probable cause and exigent circumstances. The Court held that doing so constituted an unlawful search. *See* 133 S. Ct. at 1413.

34. 133 S. Ct. 1958 (2013).

35. Under Maryland law, the police took a buccal swab from the inside of an arrestee's cheek as part of routine booking procedure for serious offenses. After receiving an analysis of the swab, the police forwarded the DNA results to the FBI, which, pursuant to federal law, maintains the Combined DNA Index System (CODIS), which allows a suspect's DNA to be compared to the DNA results of unknown suspects for other crimes. *See King*, 133 S. Ct. at 1966-68.

36. *See King*, 133 S. Ct. at 1980 (Scalia, J., joined by Ginsburg, Sotomayor & Kagan, JJ.) (dissenting) (suspicionless buccal swabbing for DNA testing authorized by Maryland law is an unreasonable search); *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment, joined by Ginsburg, Breyer & Kagan, J.J.) (relying on *Katz* and concluding that prolonged GPS monitoring of a vehicle could constitute a search); *id.* at 955 (Sotomayor, J., concurring) (expressly agreeing with Justice Alito's concurrence on this point); *Kyllo*, 533 U.S. at 29 (Scalia, J., for the Court, joined by Souter, Thomas, Ginsburg & Breyer).

37. For some additional examples, see Alex Kozinski & Eric S. Nguyen, *Has Technology Killed the Fourth Amendment?* 2010–2011 Cato Sup. Ct. Rev. 15, 18–19, 28 (2012) (radio-frequency identification tags attached to individual pieces of store-sold clothing, "smart" electric meters that identify what home device is being powered, and FasTrak or E-ZPass devices).

38. United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring in the judgment).

installed GPS software in cell phones in order to make it easier for law enforcement and emergency medical services teams to respond to 911 calls.[39] Now, however, the same tool allows law enforcement to track a person's movements as long as he or she is carrying an operational cell phone.[40] There will be considerable litigation over the circumstances in which law enforcement can obtain GPS tracking information.[41]

Predicting where the Supreme Court will take Fourth Amendment law in connection with new technologies based on the few and vague suggestions set forth in the majority, concurring, and dissenting opinions in cases such as *Kyllo, Jones, Jardines, and King* is a more hazardous undertaking than Joseph's analysis of the Pharaoh's dreams.[42] Nonetheless, there are a few predictions that can be made with a tolerable degree of certainty.

First, like a military Explosives Ordinance Disposal technician attempting to clear a minefield, the Court is likely to address new technologies deliberately, and incrementally, using the old-fashioned common law, case-by-case approach to decision making—rather than attempt to devise broad rules that would decide a large category of cases not presently before the Court.[43] Indeed, the Court has expressed a reluctance to decide more than what is necessary to resolve the particular case before it, partially because judges are not in a position to fully understand contemporary technology (let alone to

39. *See, e.g.*, "*Editorial: 'Black Boxes' Are in 96% of New Cars*," USA Today, Jan. 6, 2013, *available at* http://www.usatoday.com/story/opinion/2013/01/06/black-boxes-cars-edr/1566098/ (last visited July 25, 2013).

40. Pursuant to the Warning, Alert and Response Network Act, Pub. L. No. 109-357, 120 Stat. 1884 (2006), the Federal Communications Commission, the Federal Emergency Management Agency, the Alliance for Telecommunications Industry Solutions, and the Telecommunications Industry Association have created a collaborative project designed to inform cell phone subscribers of three types of safety threats in their vicinity: alerts issued by the President, alerts involving an immediate threat to life or safety (e.g., severe weather, chemical spills, or terrorist threats), or Amber Alerts (*i.e.*, child abductions). *See, e.g.*, Linda K. Moore, Cong. Res. Serv., The Emergency Alert System (EAS) and All-Hazard Warnings (Dec. 14, 2010). According to the FCC, the WEA project "is not designed to—and does not—track the location of anyone receiving a WEA alert." FCC, WEA Consumer Guide; *see also* Verizon Wireless, Wireless Emergency Alerts FAQs, *available at* http://support.verizonwireless.com/clc/faqs/Wireless%20Service/emergency_alerts_faq.html?grp=1&faq=16 (last visited July 25, 2013). The technology, however, permits the government to do just that.

41. The U.S. Court of Appeals for the Fifth Circuit recently held that the government can obtain information regarding a person's cell phone whereabouts from a cell phone provider under a court order without needing a search warrant. *See In re* Application of the United States of America for Historical Cell Site Data, No. 11-20884 (5th Cir. July 30, 2013). Two weeks earlier the New Jersey Supreme Court had ruled that the government can obtain that information only under a search warrant. *See* State v. Earls, No. A-53-11 (068765) (N.J. July 18, 2013).

42. *See Genesis* 41:1–36 (Joseph interprets the Pharaoh's dreams).

43. Consider Justice Kennedy's comments for the Court in City of Ontario v. Quon, 130 S. Ct. 2619, 2629–30 (2010), which involved a search of a government-issued phone:

> The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. See, *e.g., Olmstead v. United States*, 277 U.S. 438 (1928), overruled by *Katz v. United States*, 389 U.S. 347 (1967). In *Katz*, the Court relied on its own knowledge and experience to conclude that there is a reasonable expectation of privacy in a telephone booth. *See id.*, at 360-361 (Harlan, J., concurring). It is not so clear that courts at present are on so sure a ground. Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices.
>
> Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. As one *amici* brief notes, many employers expect or at least tolerate personal use of such equipment by employees because it often increases worker efficiency. See Brief for Electronic Frontier Foundation et al. 16–20. Another *amicus* points out that the law is beginning to respond to these developments, as some States have recently passed statutes requiring employers to notify employees when monitoring their electronic communications. See Brief for New York Intellectual Property Law Association 22 (citing Del. Code Ann., Tit. 19, § 705 (2005); Conn. Gen. Stat. Ann. § 31-48d (West 2003)). At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve.

anticipate future developments) or society's likely reaction to them.[44]

In that process the Court might be willing to reconsider old doctrines. Some parties have urged the Court to reconsider its precedents in light of new technologies and changed attitudes.[45] Justice Sotomayor, for one, has signaled her willingness to reconsider the so-called third-party doctrine under which a person has no reasonable expectation of privacy in information voluntarily disclosed to a third party.[46] On the other hand, Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, has indicated an unwillingness to abandon the "reasonable expectation of privacy" test adopted in *Katz* and to return Fourth Amendment law to a property rights–based approach.[47] Whether the Court goes forward, backward, or nowhere remains to be seen.

Second, the Court, in construing the Constitution, may recognize that a haunting presence—9/11—compels the Congress and the President to obtain information necessary for the defense of the nation against the type of assaults suffered on that day. The Court may come to see that the need to prevent certain potential catastrophic terrorist actions (e.g., detonation of a "dirty" bomb in a major metropolitan area) is far weightier than the need to solve a common law crime (e.g., burglary) and tips the balance in the government's favor.

The idea that the government's need for information ranges from the essential to the trivial is not a new one. Justice Robert Jackson once suggested that the Court should interpret the Fourth Amendment differently in cases involving child kidnapping and bootlegging.[48] For the most part, the Court has not accepted his suggestion,[49] and the Court has not calibrated Fourth Amendment protections according to the seriousness of the offense being investigated. The best example of that approach is the Court's 2001 decision in *City of Lago Vista*, which rejected the argument that the Fourth Amendment prohibited a warrantless custodial arrest for misdemeanors not amounting to a "breach of the peace," such as not wearing a seatbelt.[50] Perhaps the Court has been unwilling to distinguish between misdemeanors and felonies, and even among the various types of crimes denominated felonies, for Fourth Amendment

44. *See Jones*, 132 S. Ct. at 962 (Alito, J., concurring in the judgment) ("[T]he *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.").

45. *See* Alex Kozinski & Eric S. Nguyen, *Has Technology Killed the Fourth Amendment?*, 2010–2011 Cato Sup. Ct. Rev. 15, 29–30 (2012) ("The courts—and specifically the Supreme Court—must reconsider the rationale of *Hoffa* [v. *United States*, 385 U.S. 293 (1966), which held that use of undercover informants is not an unlawful search] and similar cases. Living in an interconnected world cannot be the basis for concluding that we lack an expectation of privacy as to information we disclose to third parties as a routine part of a normal day. If the courts continue to apply this rationale, then pretty much nothing will be private, and the *Katz* standard will become as unworkable as the *Olmstead* trespass standard before it.").

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

47. *Id.* at 957–64 (Alito, J., concurring in the judgment).

48. Brinegar v. United States, 338 U.S. 169, 182–83 (1949) (Jackson, J., dissenting):

> With this prologue I come to the case of Brinegar. His automobile was one of his "effects" and hence within the express protection of the Fourth Amendment. Undoubtedly the automobile presents peculiar problems for enforcement agencies, is frequently a facility for the perpetration of crime and an aid in the escape of criminals. But if we are to make judicial exceptions to the Fourth Amendment for these reasons, it seems to me they should depend somewhat upon the gravity of the offense. If we assume, for example, that a child is kidnapped and the officers throw a roadblock about the neighborhood and search every outgoing car, it would be a drastic and undiscriminating use of the search. The officers might be unable to show probable cause for searching any particular car. However, I should candidly strive hard to sustain such an action, executed fairly and in good faith, because it might be reasonable to subject travelers to that indignity if it was the only way to save a threatened life and detect a vicious crime. But I should not strain to sustain such a roadblock and universal search to salvage a few bottles of bourbon and catch a bootlegger.

49. *See, e.g.*, Florence v. Board of Chosen Freeholders of County of Burlington, 132 S. Ct. 1510, 1520-22 (2012) (declining to limit to "serious offenses" the strip search and close visual inspection of arrestees held in custody in the general inmate population).

50. 532 U.S. 318 (2001).

purposes because the Court sees that function as a legislative one. Whatever the reason, the Court has accepted an "in for a dollar, in for a dime" approach to Fourth Amendment decision making. That may change. The Supreme Court may determine that it needs to give more weight to the government's need for intelligence information in order to protect the nation against a repeat of 9/11.

And in cases involving foreign threats to national security,[51] the Court has left itself room to do just that. For example, the Court has approved certain types of warrantless and suspicionless searches that are performed not to obtain evidence for use in a criminal prosecution, but to secure information for use in other, very different contexts.[52] Recently, the Court went out of its way to limit its approval of certain government practices—DNA testing of arrestees—to parties taken into custody for "serious" offenses.[53] In coming years, the Court may find itself confronting cases involving presidential power to collect foreign intelligence.

Third, if the Court grants the federal government such unrestricted authority to obtain private information for counterterrorism uses, the Court may also decide that it needs to modify the exclusionary rule in order to limit the government's use of that evidence for only intelligence or antiterrorism purposes. That is, the Court could decide that the government may use sophisticated electronic information acquisition and analysis technology in order to protect the nation against terrorist threats, but may not use that information in an ordinary criminal prosecution unrelated to the need that justified the original search or seizure. The Court will have to sort out competing constitutional values involving both law enforcement, military, and foreign intelligence needs and the privacy of Americans.

Fourth, the Court may postpone addressing many aspects of the relationship between the Fourth Amendment and new technologies in order to see if Congress will tackle the problem by adopting a new regulatory scheme balancing information gathering needs and privacy considerations. Four justices already have made that point.[54]

On the other hand, reluctant to anger any sizeable portion of the electorate, especially one that tends to

51. In *United States v. United States District Court*, 407 U.S. 297 (1972), the Court held that the Fourth Amendment requires the government to obtain a search warrant before engaging in "domestic" or "internal" security electronic interception that would constitute a "search." *Id.* at 309–21. The Court left open, however, the question whether the same rule would apply in the case of the direct or indirect involvement of a foreign power or its agents. *Id.* at 309, 321–22. See *In re Sealed Case*, 310 F.3d 717, 742 (Foreign Intelligence Surveillance Court of Review 2002) (referring, in discussing the case under review, to the pre-Foreign Intelligence Surveillance Act (FISA) decision in *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980): "The *Truong* court, as did all the other courts to have decided the issue, held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information. It was incumbent upon the court, therefore, to determine the boundaries of that constitutional authority in the case before it. We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President's constitutional power. The question before us is the reverse, does FISA amplify the President's power by providing a mechanism that at least approaches a classic warrant and which therefore supports the government's contention that FISA searches are constitutionally reasonable.") (footnote omitted).

52. "In some circumstances, such as '[w]hen faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable.'" Maryland v. King, 133 S. Ct. 1958, 1969 (2013) (quoting Illinois v. McArthur, 531 U.S. 326, 330 (2001)). *Compare, e.g.*, Illinois v. Lidster, 540 U.S. 419 (2004) (upholding over a Fourth Amendment challenge brief stop of every motorist for questioning about a hit-and-run incident); Vernonia School Dist. 47J v. Acton, 515 U.S. 646 (1995) (same result for random drug testing of student athletes); Michigan Dep't of State Police v. Sitz, 496 U.S. 444 (1990) (same result for brief suspicionless stops of motor vehicles to determine if the driver is intoxicated); Treasury Employees v. Von Raab, 489 U.S. 656 (1989) (same result for drug testing of armed Customs Service officers); Skinner v. Ry. Labor Executives Ass'n, 489 U.S. 602 (1989) (same result for drug and alcohol testing of railroad engineers who are involved in accidents or who violate safety regulations); New York v. Burger, 482 U.S. 691 (1987) (same result for warrantless, suspicionless searches of a closely regulated business (junk yards)); Michigan v. Tyler, 438 U.S. 499 (1978) (same result for fire marshal's inspection of burned-out premises to determine the cause of a fire); United States v. Martinez-Fuerte, 428 U.S. (1976) (same result for brief suspicionless stops at highway checkpoints at or near the border to determine if the driver or occupants are illegal aliens), *with, e.g.*, Indianapolis v. Edmond, 531 U.S. 32 (2000) (holding unconstitutional city's use of drug interdiction checkpoints used to make suspicionless stops of vehicles to determine if the driver or occupants possess or are under the influence of drugs); Chandler v. Miller, 520 U.S. 305 (1997) (same result for mandatory drug testing for political candidates); Delaware v. Prouse, 440 U.S. (1979) (same result for suspicionless, discretionary vehicle stops to check the driver's license and vehicle registration).

53. *See King*, 133 S. Ct. at 1979–80 (DNA testing).

54. *See* United States v. Jones, 132 S. Ct. 945, 963–64 (2012) (Alito, J., concurring in the judgment, joined by Ginsburg, Breyer & Kagan, JJ.)

make its opinions known in the print or electronic media, Members of Congress may decide to let the federal courts make the trade-off, at least in the first instance, in order to gauge the public's response before taking a position of their own. Congress therefore might try to wait until the Supreme Court decides the Fourth Amendment issues before swooping in to shoot the survivors.

Conclusion

The Fourth Amendment was not designed to serve as a static protection against government abuse. No provision of the Bill of Rights—particularly one outlawing "unreasonable" searches and seizures—could or should be cabined to the specific historical incidents that gave it birth. That construction would render the amendment a safeguard for the peculiar historical incidents that troubled late eighteenth century Americans rather than a guarantee that law enforcement officers act reasonably today and tomorrow.

At the same time, the Framers knew that foreign nations like England possessed superior military strength and could inflict considerable damage on the new nation on land or at sea. They likely would not have found unimaginable the need to make a trade-off between liberty and security, or to reassess that trade-off as times change. Today, hostile private organizations such as al-Qaeda possess the organizational infrastructure, financial strength, and communications abilities that nations could not have imagined in the eighteenth century, and weapons of mass destruction offer terrorist cells the ability to inflict far greater damage on this country than England's Royal Army and Navy could have inflicted on us two centuries ago. Such risks should count for something when the issue is whether the government has acted "reasonably."

How will the Supreme Court make that trade-off with regard to technologies unheard of two decades ago, to say nothing of two centuries ago? Nothing is certain. We will learn the answer only as specific cases push the Court to balance the still critical needs for security and liberty.

*—**Paul J. Larkin, Jr.,** is Senior Legal Research Fellow in the Edwin Meese III Center for Legal and Judicial Studies at The Heritage Foundation.*