YALE LAW & POLICY REVIEW

Even in a Time of Terror

*Owen Fiss**

In recent decades, many changes have occurred in our system of communication, some quite startling, and yet the telephone continues to be an important part of that system. It is the means that enables us to have conversations with friends, family, and business associates increasingly located at a distance. Admittedly, many of the exchanges that once took place on the telephone now occur through e-mails, especially when the purpose is to convey information, issue a directive, or render an opinion. We still turn to the telephone, however, when a conversation is needed, for the transmission of the human voice permits direct, highly interactive, and sometimes spontaneous engagement with others.

The conversational capacity of the telephone has been enhanced by recent technological advances that permit transmission of the images as well as the voices of the parties to a conversation. Moreover, thanks to the advent of the cell phone, it has become more convenient to place or receive a telephone call. For most of the twentieth century, the telephone was a stationary device located in the home or office or in publicly accessible phone booths. Today the telephone is mobile and can be easily carried wherever one happens to be.

Engaging in a personal conversation is not like writing a diary. We may assume that the thoughts or sentiments expressed in the conversation remain with the person with whom we are speaking, but that assumption may well be mistaken. This is so even in a face-to-face encounter. The person with whom we are speaking may turn around and share the contents of that conversation with others—in fact he or she may be secretly recording the conversation for that very purpose. Although such a risk is present in a conversation conducted over the phone, this mode of communication presents yet another threat to the privacy of a conversation, and it derives from the fact that the conversation is being electronically transmitted. A third party may obtain access to that transmission, listen in, and record whatever is said.

* Sterling Professor Emeritus of Law, Yale University. I am especially grateful to Ned Hirschfeld and Michael Pomeranz for research assistance. I also benefited greatly from the discussions in the fall 2011 Yale Law School seminar on Law and Terrorism and from the papers written for that seminar by Laura Raposo, Jane Rosen, and Tyce Walters.

In the twentieth century, as the telephone became ubiquitous and telephone conversations became more commonplace, the law increasingly sought to guard against the dangers of such interceptions by a third party (which, due to the technology initially employed to transmit telephone signals, became known as "wiretapping"). Starting in 1934, Congress prohibited private parties from ever wiretapping.[1] Although there was a question whether government officials were covered by this law,[2] in 1967 the Supreme Court construed the Fourth Amendment to limit the authority of federal officials to eavesdrop in this way, requiring them to go before a judge and obtain a warrant authorizing the interception.[3]

The statutory prohibition against wiretapping by private parties remains unqualified and appears today as a fixed feature of the legal landscape. Yet the constitutional rule protecting the privacy of telephone conversations from government interceptions is now in shambles. This turn of events is in part attributable to the reluctance of the Supreme Court to fully and forcefully safeguard the values protected by the Fourth Amendment. When, in 1967, the Court first fashioned the rule requiring warrants for wiretapping, it left for another day the question whether that rule applied to wiretapping designed to protect national security.[4] In 1972, the Court moved toward a resolution of this issue by applying the warrant requirement to an individual who had been prosecuted for blowing up a CIA building in Ann Arbor, Michigan.[5] At the same time, however, the Court identified another question—whether the rule requiring a warrant applied to the gathering of foreign intelligence—and left that question unresolved.[6] To this day, forty years later, the Supreme Court has not spoken to this issue in any direct and obvious way, and has by default allowed full sway to the political branches to regulate such interceptions.

In 1978, Congress established a comprehensive scheme for the regulation of wiretapping aimed at the gathering of foreign intelligence.[7] Although this scheme required the executive to obtain the approval of a judge before engaging in wiretapping, it qualified in important ways the standards governing the is-

1. Communications Act of 1934, Pub. L. No. 73-416, § 605, 48 Stat. 1064, 1103-04 (codified as amended at 47 U.S.C. § 605 (2012)).

2. *Compare* Nardone v. United States, 302 U.S. 379, 381-83 (1937) (holding that the Act did cover federal agents), *with To Authorize Wire Tapping: Hearings on H.R. 2266 and H.R. 3099 Before Subcomm. No. 1 of the H. Comm. on the Judiciary*, 77th Cong. 17-18 (1941) (maintaining that the statute did not prohibit the distribution within the federal government of the transcript of a wiretap).

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

4. *Id.* at 358 n.23.

5. United States v. U. S. District Court (*Keith*), 407 U.S. 297 (1972).

6. *Id.* at 309 n.8.

7. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 8, 18, and 50 U.S.C. (2012)).

suance of warrants required under the Fourth Amendment. Moreover, during the last decade, as the fight against international terrorism achieved greater momentum and political saliency, these standards were further qualified, and the power of the executive to intercept telephone calls was vastly enlarged.

The enlargement of the power of surveillance began with an executive order issued in the fall of 2001, shortly after the terrorist attacks of September 11, but culminated in a statute—enacted first in 2007[8] and then again in 2008.[9] This statute severed the analytic connection between international terrorism and wiretapping and justified such surveillance as a form of foreign intelligence gathering, which included, but was not limited to, the surveillance of persons suspected of international terrorism directed against the United States. Presented as an amendment to the 1978 scheme, the 2008 statute retained the original requirement of court approval but significantly lowered—almost to a vanishing point—the standards for obtaining that approval for international telephone calls between persons in the United States and foreigners abroad.

The Supreme Court is now considering, in a suit to enjoin the implementation of the 2008 statute, whether anyone might have standing to challenge it.[10] In this Essay, I go beyond the standing issue and address the substantive dangers posed by the 2008 statute—and, for that matter, the 1978 scheme in general—to the values protected by the Fourth Amendment. Wiretapping interferes with the exercise of personal liberties essential for democratic life and thus, even in this time of terror, should be subject to the warrant requirement long proclaimed by the Supreme Court. In the wake of September 11, the temptation will of course be great to allow an exception to the warrant requirement for extraordinary crimes. I explain why that temptation should be resisted and why, even if an exception were allowed, the grant of authority in the 2008 statute should be declared invalid under the doctrine that condemns overbroad interferences with freedom.

I. The War on Terror and the Enactment of the 2008 FISA Amendments

Soon after the September 11 attacks, President George W. Bush declared a "War on Terror" and gave concrete meaning to that declaration by launching a military campaign against al Qaeda, the far-flung terrorist organization that was responsible for those attacks. He also invaded Afghanistan when that government, then controlled by the Taliban, refused to turn over Osama bin Laden and other leaders of al Qaeda who were then harbored there.

8. Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (codified in scattered sections of 50 U.S.C. (2012)).

9. FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2474 (codified at 50 U.S.C. § 1881a (2012)).

10. *See* Clapper v. Amnesty Int'l USA, 132 S. Ct. 2431 (2012) (granting certiorari).

In the context of this military campaign, President Bush issued a number of directives as Commander-in-Chief of the armed forces. The most notorious of these orders governed the treatment of persons captured on the battlefield. He determined that persons who fought on behalf of al Qaeda or Afghanistan were "illegal enemy combatants" and thus beyond the protection of the Third Geneva Convention.[11] President Bush decreed that some of these individuals were to be subject to trial before military commissions and others were to be held for prolonged, indefinite periods—until hostilities ceased—without being afforded a trial of any type. He also established, in January 2002, a prison at Guantánamo Naval Station for these very purposes.

President Bush's orders were not, however, confined to the distant battlefield or those captured on it. Some of his orders had a direct and immediate impact on the quality of life in the United States, though they, too, were issued pursuant to his powers as Commander-in-Chief. One of the most striking, issued in the fall of 2001, established the so-called "Terrorist Surveillance Program" (TSP), which directed the National Security Agency to tap international telephone calls between persons in the United States and persons abroad who were suspected of having links to al Qaeda or associated forces. The interception of these calls was not authorized by a warrant or any other form of judicial approval.

At its inception the Terrorist Surveillance Program was hidden from public view, which, given that its purpose was to catch the unwary, is not all that surprising. On December 15, 2005, however, four years after it was instituted, the program was publicly disclosed by the *New York Times*[12] and soon became the subject of a heated public controversy. Although many objections were raised to the program, the principal one arose from the failure of the President to abide by the requirements of the Foreign Intelligence Surveillance Act (FISA).[13]

FISA was adopted by Congress in 1978 in the wake of the revelations of a Senate committee, headed by Senator Frank Church, about the far-reaching and largely uncontrolled surveillance activities of American intelligence agencies. As originally enacted, the statute required the executive to obtain permission or authorization from a special court—the Foreign Intelligence Surveillance Court—before tapping the phones of agents or employees of a foreign power. The statute decreed that the membership of the court was to consist of eleven sitting federal judges specially designated for this assignment by the Chief Jus-

11. *See, e.g.*, Military Order of Nov. 13, 2001: Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism, 66 Fed. Reg. 57,883 (defining "illegal enemy combatants" while avoiding the phrase).

12. James Risen & Eric Lichtblaue, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, Dec. 16, 2005, http://www.nytimes.com/2005/12/16/politics/16program.html (correction appended).

13. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 8, 18, and 50 U.S.C. (2012)).

tice of the United States.[14] Each was authorized to act alone. Both their identities and their proceedings were to be kept secret.[15] The 1978 statute defined a foreign power to include not only a foreign nation, but also a "group engaged in international terrorism."[16] The statute further provided that foreign intelligence information included information relating to "clandestine intelligence activities," "sabotage," "international terrorism," and "the conduct of the foreign affairs of the United States."[17] The Act declared that the procedures that it established were to be the exclusive avenue for gathering electronic foreign intelligence.[18]

Bush's Attorney General, Alberto Gonzalez, defended the President's refusal to abide by the procedures of the 1978 statute.[19] Gonzalez claimed that the September 18, 2001 congressional resolution authorizing the use of military force against those responsible for the September 11 attacks had implicitly modified the provision of the 1978 statute that made it the exclusive procedure for intercepting the telephone calls of the agents of a foreign power. In Gonzalez's view, the 2001 resolution had removed any conflict between the Terrorist Surveillance Program and the 1978 FISA statute.[20]

Gonzalez did not stop there. He also denied that Congress had the power to interfere with the effort of the President to discharge his duties as Commander-in-Chief. Article II of the Constitution vests the President with the authority and responsibility to act as Commander-in-Chief and he thus has, according to Gonzalez, the authority—the constitutional authority—to override the provisions of any statute that, in his judgment, unduly interfere with the discharge of these duties. Congress cannot tell the President how to deploy the armed forces, and similarly, Gonzalez continued, Congress cannot instruct the President in

14. 50 U.S.C. § 1803(a) (2012).

15. Provision was also made for review of the decisions of individual judges by a specially designated three-judge appellate court. Given the secretive nature of the FISA proceedings, this right of review was available only to the government. *Id.* § 1803(b).

16. *Id.* § 1801(a)(4).

17. *Id.* § 1801(e).

18. 18 U.S.C. § 2511(2)(f) (2012).

19. *See Wartime Executive Power and the National Security Agency's Surveillance Authority: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 10-15 (2006), http://www.gpo.gov/fdsys/search/pagedetails.action?granuleId=CHRG-109shrg27443&packageId=CHRG-109shrg27443.

20. *Id.* at 13-14 (arguing that the 2001 resolution "must permit electronic surveillance of those associated with al Qaeda").

his efforts to gather intelligence needed for the successful completion of the military campaign against al Qaeda and its allies.[21]

This argument was part of a larger strategy of the Administration, spearheaded by Vice President Dick Cheney and his chief assistant, David Addington, to enlarge—or, in their view, recover—the constitutional prerogatives of the President to act on his own. In fact, the Administration's position on the Terrorist Surveillance Program paralleled the position it had taken on the methods that were to be used in interrogating suspected terrorists or persons accused of having links to al Qaeda. A 2002 memorandum of the Office of Legal Counsel in the Department of Justice, obviously prepared with an eye to telling the President what he wanted to hear, declared that the President could not be constrained in his choice of the methods of interrogating enemy combatants by the statute that had been passed by Congress in 1988 to implement the Convention against Torture.[22] Much of this memorandum, specifically the contrived effort to limit the reach of the statute by narrowing the definition of torture, was subsequently repudiated in December 2004 by the Department itself, once the earlier memorandum became public.[23] This new memorandum did not, however, repudiate the portion of that earlier one that denied Congress the authority to limit the power of the President, acting as Commander-in-Chief, to choose the methods to be used for interrogating suspected terrorists. The memorandum simply said that it was unnecessary to address the issue since the President had declared that he was opposed to torture.

The President did not hide behind these departmental memoranda to define the scope of his authority to interrogate suspected terrorists. In signing the Detainee Treatment Act of 2005,[24] he claimed for himself the right to act unilaterally in conducting the War on Terror, even to the point of overriding Congress. In his signing statement, the President put into doubt the efficacy of the ban on torture that, thanks to the campaign of Senator John McCain, was made a part of that measure. Bush underscored the failure of the McCain addition to provide a remedy to enforce this ban on torture and, even more importantly, Bush declared that he would not let this statutory ban interfere with the proper discharge of his duties as Commander-in-Chief.[25] He issued the statement on

21. *Id.* at 12 ("The[] inherent authorities vested in the President by the Constitution include the power to spy on enemies like al Qaeda without prior approval from other branches of Government.").

22. Memorandum from Jay S. Bybee, Assistant Attorney Gen., Office of Legal Counsel, to Alberto R. Gonzales, Counsel to the President (Aug. 1, 2002), http://www.justice.gov/olc/docs/memo-gonzales-aug1.pdf (prepared by John C. Yoo).

23. *See* Memorandum from Daniel Levin, Acting Assistant Attorney Gen., Office of Legal Counsel, to James B. Comey, Deputy Attorney Gen. (Dec. 30, 2004), http://www.thetorturedatabase.org/files/foia_subsite/pdfs/DOJOLC001109.pdf

24. 42 U.S.C. § 2000dd (2012).

25. President George W. Bush, Statement on Signing the Department of Defense, Emergency Supplemental Appropriations To Address Hurricanes in the Gulf of

December 30, 2005, soon after the *New York Times* had disclosed the existence of the TSP wiretapping program. This coincidence lent further prominence to the Attorney General's argument that, notwithstanding the purported conflict with the 1978 FISA statute, the TSP wiretapping decree constituted a lawful exercise of the President's power as Commander-in-Chief.

On the issue of wiretapping, it is not clear who had the better of the argument in resolving the conflict between the President and Congress. Article II, which enumerates the powers of the President, does say that he is Commander -in-Chief of the armed forces, but the Constitution also grants Congress war powers. Article I gives Congress the authority to declare war, make general regulations governing the armed forces, and appropriate the funds for the military. In the domain of war, many of the powers of the President and Congress are shared or overlapping and each branch can advance a claim for primacy when there is a conflict. The President speaks for the nation. Senators and Congressmen are more likely to feel the pull of the local constituencies that elect them, though those local ties may well enhance their accountability to electors and thus strengthen their authority to speak on behalf of the people.

Those who disputed the expansive conception of executive power embodied in the TSP wiretapping program made frequent reference to Justice Jackson's concurring opinion in the 1952 *Youngstown* decision.[26] In that case, the Court set aside President Truman's seizure of the steel mills, which, according to Truman, was necessary to prevent a strike by organized labor that would otherwise interfere with the United States' military effort in the Korean War. The majority opinion in *Youngstown*, written by Justice Black, held that the seizure constituted an act of lawmaking, a power belonging to Congress, and thus could not be seen as a proper exercise of the President's power as Commander-in-Chief.[27]

Justice Jackson concurred in the result, but introduced a more pragmatic scheme for defining the limits on the President's power. That power, he said, varied according to its relation to the exercise of congressional power and was at the lowest ebb when it was in conflict with an explicit statutory command.[28] Such a pragmatic approach did not, however, fully resolve the dispute between the President and Congress over the Terrorist Surveillance Program, so differ-

Mexico, and Pandemic Influenza Act, 2006 (Dec. 30, 2005), *available at* http://www.presidency.ucsb.edu/ws/index.php?%20pid=65259 (declaring that "[t]he executive branch shall construe" the prohibition "in a manner consistent with the constitutional authority of the President to supervise the unitary executive branch and as Commander in Chief and consistent with the constitutional limitations on the judicial power" in order to "protect[] the American people from further terrorist attacks").

26. *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 634-55 (1952) (Jackson, J., concurring).

27. *Id.* at 588-89 (with majority opinion).

28. *Id.* at 635-38 (Jackson, J., concurring).

ent in many respects from the seizure of steel mills. The President's power may indeed be at its weakest when it is in conflict with a statute, but Justice Jackson was careful not to deny the power of the President even under these circumstances if, as Gonzalez maintained, it lies within the constitutional grant of power to the President as Commander-in-Chief.

In the end, the nation was saved from the difficulties inherent in resolving the conflict between the President and Congress. In January 2007, after a year-long public debate about the Terrorist Surveillance Program, the Attorney General changed his strategy. He turned to the FISA court and got what he wanted. In a letter to the Chairman and ranking minority member of the Senate Judiciary Committee, the Attorney General reported that on January 10, 2007, a judge on the FISA court had issued orders—arguably ones that might be characterized as "blanket" orders—authorizing the wiretapping covered by the Terrorist Surveillance Program.[29] As Gonzalez put it, a FISA judge had issued "orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda."[30] The Attorney General also said that in light of this turn of events, the President had determined that there was no need to continue the Terrorist Surveillance Program, although the Attorney General affirmed his belief that the program "fully complies with the law."[31]

Factions within the Administration soon grew uneasy with this newly announced willingness of the Attorney General to submit to the requirements of FISA. Some objected to the scope of FISA, which had been construed to cover any communication routed through the United States, even telephone calls between two foreigners located abroad.[32] Others objected to the need to obtain court approval when people in the United States were parties to the conversation though the target of the interception was a foreigner located abroad.[33] Still

29. 153 CONG. REC. 1380-81 (2007).

30. *Id.*

31. *Id.* at 1381.

32. *Your World with Neil Cavuto* (Fox News television broadcast July 31, 2007) (transcript available at http://www.foxnews.com/story/0,2933,291763,00.html#ixzz22U84w38c (quoting John Boehner's understanding that, according to a judge, FISA "prohibit[ed] the ability of our intelligence services and our counterintelligence people from listening in to two terrorists in other parts of the world where the communication could come through the United States"); *see also* Mark Hosenball, *An 'Intel Gap': What We're Missing*, NEWSWEEK, Aug. 6, 2007, at 9 ("[I]ntel-collection officials concluded that FISA court authorizations should be obtained to eavesdrop not just on messages where at least one party is inside the country, but also for eavesdropping on messages between two parties overseas that pass through U.S. communications gear.").

33. Greg Miller, *New Limits Put on Overseas Surveillance*, L.A. TIMES, Aug. 2, 2007, http://articles.latimes.com/2007/aug/02/nation/na-spying2 (quoting officials confirming that FISA affected cases "'where one end is foreign and you don't know

others were troubled by a decision by another FISA judge, who in March 2007, when considering a renewal of the original January 10 orders, took the view that applications for authorization to wiretap under FISA had to be made on a particularized or person-to-person basis.[34] On April 13, 2007, only months after Gonzalez's compliant letter to the Senate Judiciary Committee, the Administration gave expression to this backlash and introduced legislation that would modernize FISA—or, put otherwise, give the intelligence agencies all the power they thought they needed.[35]

Congress responded favorably to the Administration's overtures, first on August 5, 2007, when it passed the Protect America Act.[36] That law was conceived as a temporary measure. By its very terms it was scheduled to expire in six months, and it in fact expired, after a short reprieve, on February 16, 2008. On July 10, 2008, Congress enacted the replacement statute.[37] It was presented as an amendment of the 1978 statute, and thus was appropriately named the FISA Amendments Act of 2008. It essentially allowed FISA judges to authorize wiretaps on the terms and conditions proposed by the Administration. This statute was originally scheduled to expire at the end of 2012, and at that time it was renewed until 2017—which is more than fifteen years after the Terrorist Surveillance Program was first instituted.[38]

II. Obama's Position on the 2008 FISA Amendments

Although the 2008 statute was sponsored by President Bush and is historically connected to the Terrorist Surveillance Program he instituted, it has been endorsed by his successor, President Barack Obama. He signed into law the re-

where the other is'—meaning warrants would be required even when it was unclear whether communications were crossing the United States or involved a person in the United States").

34. Joby Warrick & Walter Pincus, *How the Fight for Vast New Spying Powers Was Won*, Wash. Post, Aug. 12, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/08/11/AR2007081101349.html ("The decisions had the immediate practical effect of forcing the NSA to laboriously ask judges on the Foreign Intelligence Surveillance Court each time it wanted to capture such foreign communications from a wire or fiber on U.S. soil.").

35. *See* Press Release, U.S. Dep't of Justice, Fact Sheet: Title IV of the Fiscal Year 2008 Intelligence Authorization Act, Matters Related to the Foreign Intelligence Surveillance Act (Apr. 13, 2007), http://www.justice.gov/opa/pr/2007/April/07_nsd_247.html.

36. Protect America Act of 2007, Pub. L. No. 110-155, 121 Stat. 552 (codified at 50 U.S.C. §§ 1801, 1803, 1805 (2012)).

37. FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (codified at 50 U.S.C. § 1881a (2012)).

38. FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631 (codified in scattered section of 18 and 50 U.S.C.).

newal, but even before that he supported the measure. As a senator, Obama opposed a provision of the 2008 statute that gave immunity from civil suits to the telephone carriers who had participated in the original Terrorist Surveillance Program by giving the NSA access to their facilities. Obama lost that fight[39] and ultimately voted for the 2008 statute.[40] His Attorney General, Eric Holder, subsequently declared at his confirmation hearing in January 2009 that he would defend the constitutionality of the statute.[41] Soon after the 2008 statute had been signed into law, a lawsuit challenging it and seeking to enjoin its implementation was filed,[42] and this suit was pending at the time of Holder's confirmation hearing.

Holder's assurance to the senators should be seen not as a grudging recognition of a ministerial duty, but rather as the expression of the broad policy position of the Obama Administration: a willingness—perhaps a reluctant willingness, but still a willingness—to continue most of Bush's counterterrorism policies. President Obama has studiously and consistently avoided using the phrase "War on Terror," but he has repeatedly declared that the United States is at war with al Qaeda. He maintained that position even after Osama bin Laden was killed in May 2011 during an attack on his compound in Pakistan. Admittedly, on January 22, 2009, the day after his inauguration, Obama issued executive orders that sought to minimize the risk of torture in the interrogation of suspected terrorists by imposing the Army Field Manual on the CIA and closing secret prisons—the "black sites"—that the CIA had maintained.[43] He also ordered that the prison at Guantánamo be closed in a year's time.[44] Congress has blocked the implementation of this order, but the significance of the closing soon became unclear, since in May 2009, in his now-famous National Archives speech,[45] Obama embraced key Bush policies that gave rise to the notoriety of the Guantánamo prison, such as prolonged, indefinite detention without trial of some of the prisoners held there and the use of military commissions to try some of the others.

39. 154 Cong. Rec. 14,378-79 (2008).

40. *Id.* at 14,385.

41. *Nomination of Eric H. Holder, Jr., Nominee To Be Attorney General of the United States: Hearing Before the S. Comm. on the Judiciary*, 111th Cong. 104 (2009).

42. *See* Amnesty Int'l USA v. McConnell, 646 F. Supp. 2d 633 (S.D.N.Y. 2009), *vacated* 638 F.3d 118 (2d Cir. 2012), *cert. granted* 132 S. Ct. 2431 (2012).

43. Exec. Order No. 13,493, Review of Detention Policy Options, 74 Fed. Reg. 4901 (Jan. 22, 2009).

44. Exec. Order No. 13,491, 74 Fed. Reg. 4893 (Jan. 22, 2009); Exec. Order No. 13,492, 74 Fed. Reg. 4897 (Jan. 22, 2009).

45. President Barack Obama, Remarks by the President on National Security (May 21, 2009), http://www.whitehouse.gov/the-press-office/remarks-president-national-security-5-21-09.

In conducting his War on Terror, President Bush sometimes pursued an emphatic brand of unilateralism and claimed, as we saw in his defense of the Terrorist Surveillance Program, the power to act in ways that violated congressional mandates. This stance of Bush has been used to distinguish President Obama's counterterrorism strategy, but the differences may not be as great as first appears. Although Bush initially spoke defiantly, he ultimately turned to Congress, as he did with the 2008 FISA amendments, for the powers he initially claimed as Commander-in-Chief. Moreover, as Obama's first term drew to a close and the disagreements with Congress over the closure of Guantánamo sharpened, he took exception to a provision in the annual defense appropriations bill that limited his powers to transfer prisoners out of Guantánamo. In a manner reminiscent of Bush's response to McCain's ban on torture in the Detainee Treatment Act of 2005, Obama issued a signing statement in which he declared that "in the event that these statutory restrictions operate in a manner that violates constitutional separation of powers principles, my Administration will implement them in a manner that avoids the constitutional conflict."[46] In defending some of his policies, like targeted killings, Obama often pointed to the congressional resolution of September 18, 2001, which authorized the use of force against those responsible for the attacks of September 11. But this practice does not differentiate him from Bush, who, as we saw, also treated the September 18 resolution as the congressional authorization for the military campaign he began against al Qaeda and Afghanistan and thus as the foundation for his exercise of the power of Commander-in-Chief.

At the moment, the Obama Administration is trying to block judicial review of the 2008 surveillance statute by denying that the plaintiffs in the suit filed immediately after the statute was enacted have standing to challenge it.[47] The plaintiffs consist of a group of lawyers, journalists, and human rights researchers who have professional interests in the Middle East and who have regularly been in touch with persons in the region who might be thought to be terrorists. One of the lawyers represents Khalid Sheik Mohammad, the alleged

46. President Barack Obama, Statement by the President on H.R. 4310 (Jan. 2, 2013), http://www.whitehouse.gov/the-press-office/2013/01/03/statement-president-hr-4310. In the December 2011 defense appropriations bill, Congress belatedly endorsed the policy of imprisonment without trial and tried to require either trial by military commission or imprisonment without trial for all foreign nationals being held as unlawful or unprivileged enemy combatants. National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, §§ 1021-34, 125 Stat. 1298, 1562-74. In response to that measure, Obama subsequently issued "waivers" exempting broad categories of prisoners from the statute's requirements. *See* Office of the White House Press Secretary, *Presidential Policy Directive—Requirements of the National Defense Authorization Act*, WHITE HOUSE (Feb. 28, 2012), http://www.whitehouse.gov/the-press-office/2012/02/28/presidential-policy-directive-requirements-national-defense-authorizatio.

47. Clapper v. Amnesty Int'l USA, 132 S. Ct. 2431 (2012) (granting certiorari).

mastermind of the September 11 attacks, who is now being tried before a military commission at Guantánamo.[48]

The Court of Appeals for the Second Circuit found that there was a substantial risk that the plaintiffs' telephone calls would be intercepted under the authority of the 2008 statute and that, at the present time, the plaintiffs would have to adjust their action accordingly to avoid that risk, for example, by speaking in more guarded ways or traveling to the region to have face-to-face conversations with possible witnesses.[49] The Second Circuit feared that to insist upon more—namely, that the plaintiffs show that their telephone calls are in fact being intercepted or will be intercepted—would, given the secretive nature of such surveillance, mean that virtually no one would have standing to challenge the validity of the statute. Although the victim of a tap might be notified of the interception if he or she later became the subject of a criminal prosecution, such notice would hardly avoid the risk of interception and the harm caused by the statute to the entire group of plaintiffs. The Administration also pointed to provisions in the 2008 statute that gave telephone companies standing to test its validity, but once again, the Second Circuit concluded that was not adequate to protect the distinct interests of the plaintiffs.

At this juncture—arising almost four years after the statute was passed—one would have assumed that the case would be transferred to the district court for a ruling on the merits. But Obama sought review of the Second Circuit decision in the Supreme Court and oral argument was held before the Court this past October. In this Essay, I put the standing issue to one side and consider instead the validity of the 2008 statute, which the Obama Administration is fully prepared to defend when, and if, the Supreme Court decides that the plaintiffs have standing to challenge it.

III. The Origins of the Concept of "Foreign Intelligence Gathering"

The 2008 statute is unconnected to warfare. It was enacted during an era defined by the initiation of a War on Terror, but, unlike the Terrorist Surveillance Program, it has no analytic connection to the fight against al Qaeda or any other military operation launched in response to the events of September 11. As an amendment of the 1978 FISA statute, the 2008 Act is linked, not to war, but rather to the process governed by that statute—gathering foreign intelligence.

The concept of "foreign intelligence gathering" emerged as a distinct legal category in a rather odd manner—in the crevices of a back-and-forth between Congress and the Supreme Court on the rules that should govern wiretapping. The Supreme Court took the initiative in 1967, during the halcyon days of the

48. *See* Bill Mears, *Supreme Court Hears Arguments on Secret Domestic Surveillance,* CNN.com, Oct. 29, 2012, http://security.blogs.cnn.com/2012/10/29/supreme-court-hears-arguments-on-secret-domestic-surveillance.

49. Amnesty Int'l USA v. Clapper, 638 F.3d 118, 139-40 (2d Cir. 2011), *cert. granted* 132 S. Ct. 2431 (2012).

Warren Court, when it held in *Katz v. United States*[50] that the Fourth Amendment required government wiretapping to be authorized by a judicial warrant.

In taking this step, the Supreme Court rejected an approach to the Fourth Amendment, crafted by Chief Justice Taft in the late 1920s in *Olmstead v. United States*,[51] which had placed wiretapping beyond the Fourth Amendment on the theory that it was neither a "search" nor a "seizure." For the Court in *Katz*, these two words were not to be treated as Taft imagined—narrow pigeonholes into which the Court had to fit the contested executive activity. They were part of the initial phrase of the Amendment ("the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures"[52]) and this phrase, taken as a whole, should be understood as indicative of a purpose to protect the privacy of ordinary citizens. In the words of Justice Harlan's concurrence, often thought of as the authoritative gloss on what the Court had decided in *Katz*, the applicability of the Fourth Amendment, now seen in part as a protection of privacy, depends on two conditions: first, a person must "have exhibited an actual (subjective) expectation of privacy and, second, . . . the expectation [must] be one that society is prepared to recognize as 'reasonable.'"[53]

As a purely technical matter—of no interest to the Court in *Katz* or, for that matter, in any of its progeny—the case before the Court did not involve wiretapping, but something closer to eavesdropping. FBI agents had attached a listening device to the outside of a public telephone booth. The Court fully acknowledged the limited and circumspect character of the executive's action. The FBI agents had confined their eavesdropping to only six occasions when the accused was using the telephone booth and had confined their eavesdropping to a short period of time (an average of three minutes). Still, the Court ruled that this action by the executive required prior judicial authorization—the issuance of a warrant by a detached and neutral magistrate.[54]

In insisting upon a warrant, the Court was driven by an understanding that conceived of the diffusion of powers among the various branches of government as a way of protecting freedom. It also drew upon the established rules governing intrusions into the home, long thought of as the citadel of privacy. The warrant had to identify the target of the tap with particularity. It also had to be based on an application that gave, under oath, the reasons for believing that the individual had committed, was committing, or was about to commit a crime.[55]

50. 389 U.S. 347 (1967).

51. 277 U.S. 438 (1928).

52. U.S. Const. amend. IV.

53. 389 U.S. at 361 (Harlan, J., concurring).

54. *Id.* at 358 (majority opinion).

55. *Id.* at 356-57.

The Court in *Katz* carefully noted the banal character of the case under consideration. It involved the prosecution of an individual who was charged with participating in a gambling ring. The Court distinguished such a case from one involving issues of national security and specifically declined, in the penultimate footnote, to say whether warrants would be necessary in such cases. As the Court put it, "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case."[56]

In 1968, soon after the *Katz* decision, Congress, moved by a spirited public campaign to get tough on crime, passed the Omnibus Crime Control and Safe Streets Act.[57] In Title III of that measure, Congress established rules governing wiretapping. It faithfully endorsed the *Katz* requirements and prescribed the procedures for obtaining warrants for wiretapping. Yet it ended with a proviso—so similar to the *Katz* footnote—that declared that nothing in the measure should be read as requiring a warrant in national security cases.[58] The proviso specifically identified two situations that were exempted by the warrant requirements of the statute. One such situation arises when the President is seeking to protect against attack or other hostile acts of a foreign power, safeguard national security information against foreign intelligence activities, or obtain foreign intelligence information deemed essential to the security of the United States. The other situation covered by the proviso arises when the President is trying to protect against clear and present dangers to the structure or existence of the government.

The dialectic between the Court and Congress took yet another turn in 1972 when, in the so called *Keith* case,[59] the Court was called upon to consider this proviso of the 1968 Act. By this time the Warren Court had begun to disintegrate, although a new institution had not fully come into being. The majority decision was written by Justice Powell, who had recently been appointed to the Court by President Richard Nixon. Another new Nixon appointee, Justice Blackmun, joined his opinion, as did four who had supported *Katz*—Justices Douglas, Brennan, Marshall, and Stewart, who had written the majority opinion in *Katz*. The case arose from the radical politics engendered by widespread opposition to the Vietnam War and appeared on the Court's docket, "at a time," as Justice Powell acknowledged, "of worldwide ferment and . . . civil disorders."[60]

Three individuals were charged with participating in a conspiracy to destroy government property. One of the three was also charged with blowing up

56. *Id.* at 358 n.23.

57. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified in scattered sections of 5, 18, and 42 U.S.C. (2012)).

58. *Id.* § 2511.

59. United States v. U. S. District Court (*Keith*), 407 U.S. 297 (1972).

60. *Id.* at 319.

a CIA office in Ann Arbor, Michigan. In response to a pretrial motion by this individual, the Attorney General filed an affidavit in which he acknowledged that federal officials had intercepted telephone conversations in which the accused had participated. The Attorney General also acknowledged that these wiretaps were not authorized by a warrant, although he went on to insist that the interception was a reasonable exercise of the President's power to protect national security and that a warrant was not required for such interceptions.

Justice Powell began his analysis by putting Title III to one side. The proviso exempted the Attorney General from the general requirements of the statute in national security cases but was not a grant of authority. According to Justice Powell, the proviso left the Attorney General where it found him—that is, subject to the Fourth Amendment. Yet the Court, recall, had declined in *Katz* to resolve how the Fourth Amendment applies to national security cases. Justice Powell offered a partial answer to this question by drawing a distinction, arguably suggested by the proviso in Title III, between threats to national security posed by "domestic organizations"—which he referred to throughout his opinion as "domestic security matters"—and to threats to national security posed by "foreign powers or their agents."[61] He defined domestic organizations to refer to "a group or organization (whether formally or informally constituted) composed of citizens of the United States and which has no significant connection with a foreign power, its agents or agencies."[62] He then applied the Fourth Amendment warrant requirement to "domestic security matters," as he characterized the case before him. In a manner reminiscent of *Katz*, however, he also declared that he was expressing no opinion "on the scope of the President's surveillance powers with respect to the activities of foreign powers, within or without this country."[63]

The 1978 FISA statute sought to fill the decisional space left by the Court first in *Katz* and then narrowed in *Keith*. The statute established a procedure that required the Attorney General to apply to a special court for permission or authorization to intercept telephone calls—both domestic and international—that were being transmitted through facilities located in the United States. This prior court approval requirement of FISA should not, however, be confused with the warrant requirement that had been imposed by the Court in *Katz* and *Keith*. FISA did not require, as those two decisions had, that the government set forth reasons for believing that the target of the tap is guilty of a crime. The government need only set forth reasons for believing that the target of the surveillance is an agent or employee of a foreign power and that the interception is likely to secure foreign intelligence, which, recall, is broadly defined by the statute as information that could be, but need not be, related to criminal activity such as sabotage or international terrorism. By the terms of the statute, foreign

61. *Id.* at 321-22.

62. *Id.* at 309 n.8.

63. *Id.* at 308.

intelligence may also relate to alleged clandestine intelligence activities or the conduct of foreign affairs.

As a result of the 1978 statute, a dual structure emerged for wiretapping. Some taps required warrants based on probable cause; others, those specifically designed to gather foreign intelligence, did not. Remarkably, to this day—almost thirty-five years later—the Supreme Court has not ruled on the constitutionality of the FISA scheme or the dual structure it created. Yet a number of lower courts upheld the statute.[64] Those courts then faced a new quandary: could the transcript of a telephone conversation obtained through FISA procedures be admitted into evidence in criminal prosecutions?

These courts could have held that the probable cause requirement of *Katz* and *Keith* had to be satisfied whenever the result of a wiretap was to be introduced in a criminal prosecution. They chose, however, a more permissive rule and defined that rule in terms of the purpose of the interception. As long as the primary purpose of the tap was to gather foreign intelligence, the government could use the less demanding FISA procedures for obtaining court permission and then use the results of that interception in a criminal prosecution against the target of that tap even though that permission was not based upon a showing of probable cause as understood by *Katz* and *Keith*.[65]

This ruling lessened the force of the standards that the Supreme Court had enunciated in *Katz* and *Keith*, a trend that continued with a statute passed in the immediate wake of the September 11 attacks—the USA PATRIOT Act.[66] That measure provided that foreign intelligence gathering only had to be a significant, as opposed to a primary, purpose of the interception in order for the less demanding FISA procedures to govern. As a practical matter, this enabled the government to avoid the Fourth Amendment warrant requirement as understood by *Katz* and *Keith* whenever it could show a reason to believe that the target of the interception was an agent of a foreign power and that foreign intelligence would be gathered by the interception. Gathering foreign intelligence could be a significant or substantial purpose of the tap, and thus legitimate under the less demanding FISA procedures, even if the primary purpose of the interception was to gather evidence for a criminal prosecution.

IV. The Terms of the 2008 FISA Amendments

The 2008 amendments preserved the changes to FISA effectuated by the PATRIOT Act. The government need only show that the gathering of foreign

64. *See, e.g.*, United States v. Duggan, 743 F.2d 59 (2d Cir. 1984); United States v. Nicholson, 955 F. Supp. 588 (E.D. Va. 1997).

65. *See, e.g.*, United States v. Pelton, 835 F.2d 1067, 1075-76 (4th Cir. 1987).

66. Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA PATRIOT Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered sections of 8, 12, 15, 18, 20, 31, 42, 47, 49, and 50 U.S.C. (2012)).

intelligence is a significant, as opposed to a primary, purpose of the wiretap. The 2008 statute also continued the original FISA requirements for authorizing wiretaps in which the target is a person located in the United States. In these cases, the government must, in addition to the significant-purpose showing, establish a reason for believing that the target is an agent or employee of a foreign power. However, the 2008 statute introduced a further complexity in the FISA structure by establishing, as the Bush Administration proposed, a special set of rules to apply when the target of the tap is located outside the United States.

Some of these persons abroad may be Americans or, in the language of the statute, "United States persons," a category defined to consist of United States citizens and persons lawfully admitted for permanent residence in the United States.[67] With respect to them, as with Americans within the United States, the requirements for surveillance are in accord with the original FISA statute as amended by the PATRIOT Act. The government must establish that a significant purpose of the tap is to gather foreign intelligence and that the individual is an agent or employee of a foreign power. These requirements apply regardless of whether the interception is effectuated through facilities located in the United States or through facilities located abroad.

However, in the case of non-United States persons—in my terms, foreigners—who are located abroad, the 2008 statute radically departs from the original FISA standards. As under the original statute, there is no need to obtain authorization of any kind from a FISA judge when the wiretap does not require access to facilities located in the United States.[68] When, however, the tap aimed at foreigners abroad requires access to facilities in the United States, permission by a FISA judge is required, but the traditional FISA standard is drastically lowered. Although the government must state that a significant purpose of the tap is to gather foreign intelligence, little more is required. The government need not have reason to suspect that the targets of the tap are agents or employees of a foreign power, only that they are foreigners and that they are located outside the United States.[69]

The 2008 Act not only lowers the standards for authorizing wiretaps aimed at specific or individual foreigners abroad. It also facilitates the issuance of "blanket" authorizations for taps of such persons, as the original TSP did.[70] Even though the entire FISA procedure is secretive, the 2008 Act relieves the

67. *See* FISA Amendments Act of 2008, Pub. L. No. 110-261, § 701, 122 Stat. 2436, 2437 (codified at 50 U.S.C. § 1881 (2012)).

68. 50 U.S.C. § 1802(a)(1) (2012).

69. *Id.* § 1881a(a)-(g).

70. *See* William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 18 Tex. L. Rev. 1633, 1635 (2010) ("The [2008 statute] codified a procedure to permit broad, programmatic surveillance focused on patterns of suspicious activities and not on a specific individual or the contents of their communications through changes in FISA that overcame the case-specific orientation of the original statute.").

government of the need to disclose to a FISA judge the identity of each individual to be targeted. It only requires that the government describe and employ procedures reasonably designed to ensure that its proposed surveillance activity will only target foreigners abroad.[71] Arguably, this might permit the government to obtain authorization from a FISA judge to tap the telephone calls of an entire group of foreigners abroad (e.g., "persons suspected of links with Al Qaeda" or "high-ranking officers of the Pakistani army").

All applications for warrants, even those required by *Katz* and *Keith*, are considered by a judge without notice to the target. The hope is that a judge, acting on his own, will scrutinize the factual basis of the application. This hope arguably persisted even under the original FISA scheme, though two of its features lessened the likelihood of that hope ever being realized—the judges on the FISA court are handpicked by the Chief Justice and assured a degree of anonymity. But the 2008 Act went further and sought to eliminate the powers of a FISA judge to challenge the factual predicates of the government's application for authorization for a wiretap where the target is a foreigner abroad.

In 2004, Congress passed a statute establishing the Office of the Director of National Intelligence to coordinate and oversee the work of all of the intelligence-gathering agencies of the United States.[72] This statute also amended the original FISA statute to require that those applications that had to be jointly authorized by the Director of the CIA and the Attorney General now had to be authorized by the Director of National Intelligence and the Attorney General.[73] The 2008 FISA amendments continued this requirement of joint authorization by the Attorney General and the Director of National Intelligence.[74] These officials must jointly establish a plan for governing these surveillance activities aimed at foreigners abroad, submit that plan to the FISA judge, and certify that the new FISA requirements for such targets are met.[75] In another radical departure from the original FISA scheme, the 2008 statute goes on to provide that the judge must approve the application if the certification "contains all the required elements."[76] There is no room for the judge to scrutinize, as he might or should have done in the past, the factual predicates of the government's FISA application. The 2008 statute also places a strict limit—thirty days—on the time the FISA judge has to consider the application.[77]

Having minimized the role of the judiciary, the 2008 statute provides for a measure of after-the-fact review of the surveillance activities of the Department

71. 50 U.S.C. § 1881a(a)-(g).

72. Intelligence Reform and Terrorism Protection Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (codified in scattered sections of 42 and 50 U.S.C. (2012)).

73. *Id.* § 1071(e).

74. 50 U.S.C. § 1881a(a).

75. *Id.* § 1881a(a)-(g).

76. *Id.* § 1881a(i)(3).

77. *Id.* § 1881a(i)(1)(B).

of Justice and the various intelligence agencies that might be engaged in wiretapping. This review power was entrusted to a bevy of inspectors general, who on any account are administrative officials, not detached and impartial magistrates. Inspectors general are appointed by the President and subject to removal by him. The Senate must confirm their appointment and be given thirty days notice of their removal.[78] They were created by a 1978 statute, also a response to the disclosures of the Church committee, and were charged with reporting to Congress and the executive on the practices of the administrative agencies to which they are assigned. The 2008 FISA amendments specifically instructed the Inspector General of the Department of Justice and his counterpart in each of the intelligence agencies involved in the surveillance to review and report on the extent to which the surveillance targets persons ultimately determined to have been located in the country, and the extent to which the surveillance produces intelligence reports that identify Americans.[79]

V. The Conflict with the Fourth Amendment

The constitutional protection of privacy is not absolute. The Fourth Amendment does not altogether deny the government access to the information that it needs to discharge its elemental duty to secure the land. Rather, it seeks to minimize or avoid the dangers inherent in surveillance by restricting the techniques and methods that the government may employ to acquire that information. It places a zone around domains and activities of the individual—those endowed with a "reasonable expectation of privacy"[80]—and then constructs a barrier to protect this zone. This barrier is reinforced by the understanding that each intrusion not only impairs the individual's interest in privacy and thus undermines the conditions necessary for human flourishing, but also may, given the particular circumstances of the intrusion and the reasons for it, threaten a multitude of other interests, including those protected by the constitutional guarantees of free speech, fair trial, and equal treatment.

The 2008 FISA amendments are a grant of authority. They allow the government to intercept telephone conversations and thus to interfere with an activity most certainly endowed with a reasonable expectation of privacy. The validity of the statute turns on the conditions it imposes on the exercise of this authority and whether those conditions are stringent enough to comport with the Fourth Amendment and the barriers it interposes against such intrusions of privacy. Typically, the Fourth Amendment has been used to review criminal convictions, and in that context constitutes a standard to measure the investigatory activity of law enforcement officials. It also has been held to establish a standard to measure legislative grants of investigative authority and the power

78. Inspector General Act of 1978, 5 U.S.C.A. App. 3 (2010).

79. 50 U.S.C. § 1881a(*l*)(2).

80. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

of government officials to engage in various forms of surveillance, including wiretapping.[81]

A. The Probable Cause Requirement

The barrier constructed by *Katz* and *Keith* has two features. It requires court approval prior to the interception and it conditions that approval upon a showing of probable cause. FISA—as originally enacted and as amended—satisfies the first requirement of prior court approval. But it qualifies in important ways the second—the need to show probable cause.[82]

The Fourth Amendment does not elaborate on the meaning of probable cause, but, as *Katz* and *Keith* and countless other cases declared, probable cause is, as used in the Fourth Amendment, a technical term linked to criminality. It does not simply mean reason to believe, but rather reason to believe that the person whose calls are being intercepted had committed a crime, is committing a crime, or is about to commit a crime.[83]

The burden of showing probable cause may weigh heavily on the government. The government may sometimes need to wiretap in order to acquire the information that will enable it to identify a criminal, or give it reason to believe that an individual is about to commit a crime. The same could be said about

81. For example, in *Berger v. New York*, 388 U.S. 41 (1967), the Supreme Court overturned a bribery conviction based on evidence obtained without a warrant that met the Fourth Amendment standards of particularity. The Court also declared unconstitutional on its face the New York statute that established the scheme governing electronic surveillance under which the warrant was issued for failing to include a sufficient particularity requirement.

82. Some have suggested that FISA's qualification of the probable cause requirement does not go far enough, and that further qualification or even elimination of that requirement would improve the statute (or replacement legislation). *See, e.g.*, Stephanie Cooper Blum, *What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, 18 B.U. PUB. INT. L.J. 269, 291-94, 308-12 (2009).

83. A contrary understanding of the related term "individualized suspicion" recently surfaced in footnote 2 of Justice Scalia's opinion for the Court in *Ashcroft v. Al-Kidd*, 131 S. Ct. 2074 (2011), a case that involved an arrest under the federal material witness statute. In her concurrence, Justice Ginsburg argued that the "individualized suspicion" needed for a warrant is a legal term of art that means suspicion of wrongdoing. *Id.* at 2088 n.3 (Ginsburg, J., concurring). Justice Scalia, however, used the term more loosely and concluded that the material witness warrant in the case had been properly based on "individualized suspicion" that the target possessed relevant information about others. *Id.* at 2082 n.2. He said: "No usage of the word is more common and idiomatic than a statement such as 'I have a suspicion he knows something about the crime,' or even 'I have a suspicion she is throwing me a surprise birthday party.'" *Id.* No authority was offered in support of the view—so odd for an originalist—that this contemporary or idiomatic usage was intended by the Framers in the Fourth Amendment context.

intrusions into the home. They may be needed to establish probable cause. However, under the Fourth Amendment, that information must be secured by means that do not entail intercepting a conversation or intruding into a domain that is endowed with a reasonable expectation of privacy. In *Katz* and again in *Keith*, the Supreme Court stopped short of applying this understanding of probable cause to wiretapping aimed at gathering foreign intelligence and reserved that question for another day—a day that has not yet come.

As a purely predictive matter, it is difficult to say that the Court will take the additional step and apply to FISA wiretaps—either as originally enacted in 1978 or amended in 2008—the understanding of probable cause announced in *Katz* and *Keith*. The present Court might even, on the worst of days, overrule those decisions. But my inquiry is not predictive, but rather normative — what would a fair-minded lawyer, acting as a member of civil society, say? From that perspective, the additional step seems necessary. It is difficult to understand how the term "probable cause" could be given different meanings depending on the type of information sought, the purpose of the government in seeking this information, or the citizenship and location of the person who is the target of the interception.

The 2008 statute varies the conditions for obtaining court approval depending on the purpose of the surveillance and the citizenship and location of the target, though in no instance does it require the suspicion of criminality that is the essence of probable cause. In all FISA wiretaps, the government must show that a significant purpose—not the only purpose, nor even the primary purpose—of the interception is to gather foreign intelligence, which of course may have no connection to any suspected criminal activity.[84] The statute imposes a further condition on obtaining court approval when the target of the tap is an American citizen or a person who is lawfully in the United States: the government must show that the target is an employee or agent of a foreign power.[85] If the foreign power is an international terrorist organization, it can be fairly assumed that there is reason to believe that the target is a terrorist and thus that the probable cause requirement has been satisfied. But wiretapping is allowed under FISA even if the foreign power is another nation, for example the United Kingdom or Saudi Arabia, and there is thus no reason to suspect the target of criminal activity.

There is an even more striking departure from the requirements of probable cause when the target is a foreigner abroad. In those cases, there is no need to show even that the target is an employee or agent of a foreign power, only that he or she is a foreigner abroad. Moreover, in these cases, the FISA judge is denied the capacity, present in any probable cause hearing, of scrutinizing the factual basis of the government's application. On top of that, the 2008 amendments authorize a FISA judge to approve "blanket" wiretaps aimed at groups or categories of persons consisting of foreigners abroad—once again sharply at va-

84. *See supra* note 17 and accompanying text.

85. *Id.* § 703 (codified at 50 U.S.C. § 1881b).

riance with the constitutional concept of probable cause, which requires suspicion of criminality and thus must, of necessity, proceed on an individual or person-by-person basis.

Soon after the enactment of the 2008 FISA amendments, a lawsuit—the one now before the Supreme Court on the issue of standing—was filed challenging the statute. The lawsuit was designed to focus attention on the provisions of that statute regarding foreigners abroad—and with good reason. Those provisions mark the clearest and most disturbing departure from the Fourth Amendment's probable cause requirement. Yet in fashioning these provisions, President Bush and Congress may have been relying on a 1990 decision of the Supreme Court, *United States v. Verdugo-Urquidez*,[86] which arguably could have been read as placing foreigners abroad in a constitutional free fall.

In that case, Chief Justice Rehnquist denied the protection of the Fourth Amendment to a Mexican citizen who had been forcibly taken to the United States to stand trial on drug charges and whose home in Mexico had been searched by United States drug enforcement officials without a warrant. According to Rehnquist, the Fourth Amendment—and perhaps the entire Bill of Rights—provides no protection to persons lacking a voluntary connection to the United States and thus did not govern in any way the search of the Mexican citizen's home in Mexico.[87] In saying this, Rehnquist sought to repudiate the understanding that prevailed during the Warren Court era that viewed the Constitution as imposing restraints on American officials wherever they acted and independent of the target of their actions.[88] This understanding was based on a generous reading of the 1957 decision of the Supreme Court in *Reid v. Covert*,[89] which Rehnquist went out of his way to discredit and overrule.[90]

Rehnquist's opinion was denominated the "Opinion of the Court," but it needed Justice Kennedy's support to achieve that status. Justice Kennedy, then a relatively new appointee, wrote a separate opinion in which he said that he joined the Chief Justice's opinion but in fact advanced a more cosmopolitan conception of the Constitution.[91] He brushed to one side Rehnquist's emphasis upon the prefatory words of the Fourth Amendment—"the right of the people."[92] According to Kennedy, those words were nothing more than a rhetorical flourish, a way of emphasizing the importance of what was to follow rather than a means of restricting to Americans the protection of the right guaranteed. Kennedy conceded that it would be impractical to require federal

86. 494 U.S. 259 (1990).

87. *Id.* at 274-75.

88. *See* Owen Fiss, *The War Against Terrorism and the Rule of Law*, 26 O.J.L.S. 235 (2006).

89. 354 U.S. 1 (1957).

90. *Verdugo-Urquidez*, 494 U.S. at 269-70.

91. *Id.* at 275 (Kennedy, J., concurring).

92. *Id.* at 276-77.

officials acting abroad to be subject to the same requirements as imposed on them when they are acting within the United States. For that reason, they are not, according to Kennedy, subject to the warrant requirement of the Fourth Amendment.[93] On the other hand, he continued, they are always subject to the obligation to act fairly or, in the framework of the Fourth Amendment, "reasonably."[94] Kennedy concurred in Rehnquist's outcome, but only because he felt that the federal officials had in fact acted reasonably.

Similar strains of pragmatic cosmopolitanism might be found in Justice Kennedy's opinion, this time for the majority, in the 2008 decision in *Boumediene v. Bush*.[95] In this case, Kennedy declared unconstitutional a provision of a federal statute (the Military Commissions Act of 2006) that was applied to deny access to the writ of habeas corpus to foreign nationals being detained in Guantánamo. He concluded that the statute constituted an unlawful suspension of the writ of habeas corpus. In so doing, he repudiated an effort by Congress, similar to the one embodied in the 2008 FISA amendments, to free the executive engaged in a War on Terror from constitutional constraints on its treatment of foreign nationals located abroad, though in this instance by denying them access to the writ of habeas corpus to test the legality of their detention. On the surface of his opinion, Kennedy appears to have been moved less by a regard for the rights of the prisoners than one for separation of powers—the need to preserve the capacity of the judiciary to review the legality of executive detentions. Yet the consequence of his action for the rights of Guantánamo prisoners—all foreign nationals detained abroad—was manifest and thus the *Boumediene* decision can also be read as extending the reach of the Constitution to foreigners abroad.

We need not, however, enter into the debates generated by these readings of Justice Kennedy's opinions, for even if we adopt Chief Justice Rehnquist's position in *Verdugo-Urquidez* and restrict the protection of the Fourth Amendment in the way he suggests, there is good and sufficient reason to be concerned with the surveillance authority granted the executive by the 2008 statute over telephone calls of foreigners abroad. Americans may well be parties to those calls and the interception of those calls will interfere with their reasonable expectation of privacy. In my view, the focus should not be restricted to the target of the interception, but rather should embrace all the parties to the conversation.

The 2008 amendments require court authorization of a tap aimed at foreigners abroad only when the interception entails access to facilities located in the United States. Although sometimes a conversation between two foreigners located abroad may be routed through facilities in the United States, this is rare. Presumably, the bulk of international telephone calls routed through the United States involve at least one party who is in the United States. Some of these per-

93. *Id.* at 277-78.

94. *Id.*

95. 553 U.S. 723 (2008).

sons may be transitory visitors or even persons in the country illegally and thus beyond the protection of Rehnquist's Fourth Amendment. But more likely than not, they will be United States citizens or persons lawfully granted residence in the United States—persons who had the voluntary connection to the United States that Rehnquist demanded in *Verdugo-Urquidez*.

Accordingly, a wiretap authorized by a FISA judge that is aimed at a foreign national living abroad will, in all likelihood, give the government access to private conversations of persons unquestionably entitled to the protection of the Fourth Amendment. This is indeed true of the plaintiffs in the standing case now before the Supreme Court—journalists, lawyers, and human rights researchers whose work necessitates frequent and regular telephone calls to people in the Middle East. These individuals may not in fact be the target of the surveillance and, for that reason, may be characterized, as a purely technical matter, as incidental victims of the surveillance, but there can be no mistake that they are victims of the surveillance. Just as much of their personal or private information may be acquired as that of foreign nationals living abroad. They will be fearful of speaking fully and freely or may be discouraged from using the phone altogether.

Admittedly, in the ordinary law enforcement context, probable cause must be shown for the target, but not for all the parties to the conversation. Statements by anyone who engages in a telephone conversation with the target might be used by the government in a criminal prosecution.[96] The 2008 FISA amendments might be viewed as following a similar rule, but in truth the dangers are much greater. The target of the interception need not be an individual; it might consist of groups or categories of foreign nationals, and there is no need to establish, with respect to the target, the probable cause contemplated by *Katz* or *Keith*. The government need only give reasons for believing a target is a foreigner located abroad and that a significant purpose of the interception is to gather foreign intelligence. The threshold for interception is thereby lowered dramatically and, as a consequence, the so-called incidental victims—United States citizens or lawful permanent residents of the United States—are more exposed than ever to interceptions of their private conversations.

In criticizing the 2008 amendments and perhaps the 1978 FISA scheme in general for failure to abide by the probable cause requirement of the Fourth

96. *See, e.g.*, United States v. Perillo, 333 F. Supp. 914, 919-21 (D. Del. 1971) (citing Alderman v. United States, 394 U.S. 165, 175 n.10 (1969)) (deeming constitutional the government's use of conversations between the target of surveillance and a third party in a subsequent criminal prosecution of the third party, where the surveillance was conducted pursuant to a warrant applying only to the target of surveillance and the government had made no prior probable cause showing regarding the third party); *see also* United States v. Kahn, 415 U.S. 143, 157 (1974) (holding that the government's interception of incriminating telephone calls by the wife of a target of surveillance, and the subsequent use of those calls in a criminal prosecution against the wife, did not violate the Fourth Amendment even though the government had not established probable cause regarding the wife before beginning surveillance).

Amendment, I am making little—perhaps too little—of the considered judgment of Congress and the President over the meaning of that crucial term. It is difficult, however, to endow the decisions of the President and Congress with the normative force that derives from our democratic commitments and for that reason defer to their judgment. Probable cause is a technical term and the meaning that the political branches have given to it can only be found in long and complicated statutes not easily accessible or understood by the general public, or maybe even by their representatives. Moreover, the burden of the FISA scheme—dilution or abrogation of the probable cause requirement—is in large part, though not entirely, shouldered by persons who are not entitled to participate in the electoral process. This is particularly true of the 2008 statute and its grant of authority to target the telephone calls of foreigners located abroad. Granted, the President and Congress are coordinate branches of government also charged with the duty of giving concrete meaning to the Constitution. But they are not bound by the strictures of public reason—above all, the rule requiring judgment based on principle—that gives the judiciary the authority to interpret the Constitution and, if need be, to override the interpretations of the political branches.[97]

B. The "Special Needs" Exception

The Fourth Amendment has an unusual grammatical structure. As Justice Kennedy's concurrence in *Verdugo-Urquidez* makes evident, the Amendment consists of two clauses. The first clause proclaims the right of the people to be protected against unreasonable searches and seizures.[98] The second, joined to the first by the word "and," sets forth the requirements for warrants.[99] Some scholars have advanced a disjunctive reading of the two clauses, arguing that in the minds of the Framers, the Warrant Clause sought to limit the availability of warrants, not to make their issuance decisive in determining whether an interception is, within the meaning of the first clause, reasonable.[100] The possession of a valid warrant, the argument goes, would provide an absolute defense for a

97. *See* Owen Fiss, *Between Supremacy and Exclusivity*, *in* THE LEAST EXAMINED BRANCH: THE ROLE OF LEGISLATURES IN THE CONSTITUTIONAL STATE 452, 452-67 (Richard W. Bauman & Tsvi Kahana eds., 2006).

98. 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 . . . .").

99. *Id.* ("[A]nd 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.").

100. *See, e.g.*, AKHIL REED AMAR, THE CONSTITUTION AND CRIMINAL PROCEDURE: FIRST PRINCIPLES 31-45 (1998); Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 762, 774 (1994). *But see* Carol S. Steiker, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820 (1994).

government official subsequently accused of conducting an unreasonable search. By tightly prescribing the requirements of a valid warrant, the Fourth Amendment sought to limit the issuance of warrants—and, correspondingly, the availability of an absolute defense—for unreasonable searches.

This understanding of the Warrant Clause may indeed be a plausible account of the historic origins of this provision, but even so, it does not undercut the now-ancient rule—affirmed by *Katz* and *Keith* in the context of wiretapping—requiring that if at all possible the government seek a warrant before conducting a search, and further that the warrant be issued only if certain requirements—including the showing of probable cause—are satisfied. Indeed, this rule may well be a fair implication from the bar on the defensive use of warrants that do not meet the specified standards. Liability rules often reflect an understanding of best practices.

In *Katz* itself, the Court acknowledged two very narrow exceptions to the warrant requirement: one for searches conducted in the course of an arrest, and the other for searches conducted in "hot pursuit" of a suspected criminal.[101] The Court concluded that neither exception was applicable to wiretapping and showed no inclination to create another exception.[102] In recent decades, however, the number of cases in which an exception to the warrant requirement has been made—the most familiar involves the searches of passengers and their luggage at airports[103]—has grown. These exceptions are now grouped under the heading of "special needs"[104] and have typically been justified on the ground that the intrusion of privacy is momentary, obtaining a warrant before the search is not remotely practical, and redress of abuses of power may be obtained through an action for damages.

These conditions are clearly not satisfied by FISA wiretaps. Such surveillance is not a momentary intrusion, but lasts for a considerable period of time. Under the 2008 amendments, for example, the tap can last for a year.[105] Nor can it be claimed that obtaining a warrant prior to the surveillance is a practical impossibility.[106] In contrast to airport searches, the 2008 statute requires the gov-

101. Katz v. United States, 389 U.S. 347, 357-58 (1967).

102. *Id.*

103. *See, e.g.*, United States v. Edwards, 498 F.2d 496, 499-500 (2d Cir. 1974).

104. Justice Blackmun introduced the phrase in *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring in the judgment). *See also* MacWade v. Kelly, 460 F.3d 260, 268 (2d Cir. 2006) (acknowledging that *United States v. Edwards* exemplifies what later came to be known as the "special needs exception").

105. 50 U.S.C. 1881a(a) (2012).

106. Although the Attorney General and Director of National Intelligence must ordinarily wait for a judicial order before authorizing surveillance, the 2008 FISA amendments permit the institution of a wiretap without a judicial order where the Attorney General and Director determine that "exigent circumstances" exist. *Id.* § 1881a(c)(2); *see also id.* § 1881a(a) (granting the Attorney General and Director the ability to authorize surveillance). In such cases, the Attorney General and Di-

ernment to first seek judicial approval of the interception[107]—the only issue is what must be shown to obtain that permission. Moreover, given the secrecy requirements of FISA interceptions, a retroactive action for damages for abuses of executive power is not a viable alternative. Secrecy is no bar to the work of the inspectors general, but they are only administrative officials and their task is to report on whether the practices of the executive comported with the statutory requirements, not with the constitutional standard of probable cause or any of its cognates. Their job is not to provide a remedy for such abuses, but rather to report to the executive and Congress on the extent to which surveillance has targeted or led to intelligence reports mentioning persons in the United States.

Under Title III, the government is required to give all subjects of a wiretap notice of an interception after the surveillance is complete. There is no such notice requirement in FISA. In the standing case now before the Supreme Court, the government indicated that individuals would be provided notice of an interception when the government intends to use that interception as part of a criminal prosecution.[108] Although the terms and conditions of that notice remain unclear to me, let us assume that as a result of this promised notice an individual might, now and then, learn that he or she had been the subject of a FISA tap. Then that individual might be able to demonstrate in a subsequent action for damages that the surveillance was undertaken for the worst of reasons, for example, to make life difficult for a political enemy or to learn of the accused's strategy in an ongoing criminal prosecution.

But this imagined scenario hardly lives up to one of the assumptions underlying the special needs exception: namely, that a retrospective action for damages might hold the government accountable and thus avoid unreasonable infringements of privacy. The receipt of the promised notice for a FISA tap is likely to be a rare and isolated event, available only if a criminal prosecution is launched against the individual. In any event, such notice does not adequately guard against the principal harm of wiretapping—the fear of being heard by others. This fear might limit conversations, or discourage them altogether, which would be a tremendous loss for the individual and impair the democratic character of society, though it is not likely to be a sufficient basis for an action for damages.

rector must submit a certification for the interception within seven days of its commencement, if such a certification is not already pending. *Id.* § 1881a(g)(1)(B).

107. *Id.* § 1881a(g)(1)(A).

108. Transcript of Oral Argument at 4, Clapper v. Amnesty Int'l USA (Oct. 29, 2012) (No. 11-1025), http://www.supremecourt.gov/oral_arguments/argument_transcripts/11-1025.pdf (remarks of Solicitor Gen. Donald Verrilli, Jr.) ("Your Honor, under the statute, there are two clear examples of situations in which the individuals would have standing. The first is if an aggrieved person, someone who is a party to a communication, gets notice that the government intends to introduce information in a proceeding against them."); *see also id.* at 42-43.

C. Extraordinary Crimes and the Problem of Overbreadth

In an era that began with the terrorist attacks of September 11, 2001, the temptation is great to develop special rules for surveillance activities aimed at preventing further terrorist attacks. These rules would free the government from the Fourth Amendment warrant requirement and might be justified in terms of the magnitude or severity of the harm to be avoided. They might be understood as an expansion of the special needs exception, which is premised on the disjunctive reading of the two clauses of the Fourth Amendment that makes reasonableness the touchstone of legality. The test is not whether the surveillance is authorized by a warrant showing probable cause, but rather whether the government's action is unreasonable. In a recent case, *United States v. Jones*,[109] Justice Alito suggested yet another way of conceptualizing these special rules, though the result would be the same—no warrant would be required. For Alito, the Fourth Amendment does not protect privacy, but only a reasonable expectation of privacy and the severity of the harm to be avoided would enter into the judgment as to whether there was a violation of that expectation.[110] When investigating extraordinary offenses, there may be, according to Alito, no intrusion of a reasonable expectation of privacy, and thus no warrant would be required.[111]

In the *Jones* case, the police had installed a GPS (Global Positioning System) tracking device in the undercarriage of a suspect's car without first obtaining an adequate warrant. The device was used to track the vehicle's movement over the next twenty-eight days.[112] Justice Scalia wrote the opinion for the Court and in it he applied a methodology reminiscent of Chief Justice Taft's decision in *Olmstead*. Scalia first said that the car was an "effect" within the meaning of the Fourth Amendment and then concluded that the act of installing the GPS device constituted a trespass and thus was a "search" or "seizure" within the meaning of that Amendment.[113] Justice Alito wrote a special concurrence in which he disassociated himself from Justice Scalia's mode of analysis. Condemning the police practice within the framework of *Katz*, Alito maintained that the police had violated a reasonable expectation of privacy and thus were required to obtain an appropriate warrant authorizing the surveillance.[114]

In insisting upon such a warrant, Justice Alito emphasized the length of the surveillance—twenty-eight days.[115] He thought that relatively short-term monitoring of a person's movement on a public street might be in accord with "ex-

109. 132 S. Ct. 945 (2012).

110. *Id.* at 957-64 (Alito, J., concurring in the judgment).

111. *Id.*

112. *Id.* at 948 (majority opinion).

113. *Id.* at 949-53.

114. *Id.* at 958, 964 (Alito, J., concurring in the judgment).

115. *Id.* at 964.

pectations of privacy that our society has recognized as reasonable."[116] In restating this conclusion, however, Alito also made the nature of the offense relevant for determining whether there was interference with a reasonable expectation of privacy and thus whether a warrant was necessary. As he put it: "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[117] In saying this, Justice Alito appears to contemplate a special rule for exceptional or extraordinary offenses. Mindful of the novelty of this approach, however, and perhaps in an effort to satisfy the other Justices who joined his opinion—Justices Breyer, Ginsburg, and Kagan—he ended his opinion with this disclaimer, so evocative of the national security disclaimer in *Katz* and the foreign intelligence gathering disclaimer in *Keith*: "We also need not consider whether prolonged GPS monitoring in the context of investigations involving extraordinary offenses would similarly intrude on a constitutionally protected sphere of privacy."[118]

The defendant in *Jones* was charged with drug trafficking—surely not an extraordinary offense. Terrorist activities on the scale of the 9/11 attack or any other acts of international terrorism may have that quality of extraordinariness to which Justice Alito referred. My inclination, however, is to resist the temptation to allow an exception to the warrant requirement for so-called extraordinary crimes, regardless of how the exception is formulated. It may be difficult to identify the criteria needed to implement such a distinction, but my concern with this approach runs deeper.

For one thing, I fear that an exception to the warrant requirement for extraordinary crimes would be susceptible to great abuse. The government can always claim that it is seeking to prevent an extraordinary crime and then defend that claim on the basis of knowledge that it alone has. Even more, I fear the jurisprudential consequences of such an approach. It would impair the authority and near-sacred quality of the Constitution as a charter establishing the structure of government and defining the highest ideals of the nation. It would also put judges into the business of making exceptions to a standard rule that is not easily cabined and that is at odds with their obligation to say what the law is. Pragmatic considerations often enter into judicial judgments, but never in a way that permits disregard for a clearly established constitutional command or interpretation.

However, even if Justice Alito has his way and an exception to the Fourth Amendment warrant requirement were allowed for extraordinary offenses, it is hard to see how it might save the 2008 statute, or even the FISA scheme in general. These statutes, in contrast, say, to President Bush's Terrorist Surveillance Program, are in no way limited to surveillance that is aimed at al Qaeda or associated forces, or even international terrorism in general. As originally enacted, the 1978 FISA statute defined a foreign power to include a group engaged in in-

116. *Id.*

117. *Id.*

118. *Id.*

ternational terrorism and then defined foreign intelligence in a way to include information about international terrorism. Yet the statute is not confined to terrorism. In 2004, FISA was amended to include suspected terrorists who acted on their own,[119] but that only broadened the reach of the statute.

In utilizing the powers granted by the 2008 statute, the Attorney General may be guided by an understanding of the historical context in which the statute was enacted—it was passed during an era defined by the War on Terror, and in essence sought to give legislative authorization for President Bush's Terrorist Surveillance Program. Under these circumstances, the Attorney General might well decide to use the grant of authority conferred on him only for the purpose of preventing international terrorism or pursuing those who have engaged in such terrorist activities. But we can never be sure of that. The FISA regime—as originally enacted and amended in 2008—reaches more broadly and thus exacts a toll on our freedom. The very existence of the statute gives rise to the fear that international telephone calls will be tapped without the kind of judicial scrutiny and authorization required by the Fourth Amendment.

In the context of the First Amendment and its guarantee of freedom of speech, we have learned to judge statutes on their face—on the basis of all their possible applications. Under the so-called overbreadth doctrine, the Court will strike down statutes that arguably may have some constitutionally permissible applications if there are a substantial number of applications that impinge on activities that are concededly constitutionally protected.[120] The Court will declare the statute invalid on its face as a way of enlarging the freedom of citizens to participate in those activities that are constitutionally protected. Legislators remain free to prohibit the activities that may be constitutionally unprotected, but only in a way that narrowly targets those activities and thus economizes on the sacrifice of First Amendment freedoms.

A similar doctrine needs to be recognized in the Fourth Amendment context.[121] In the First Amendment context, the overbreadth doctrine was announced as a protection against the chilling effect of a criminal statute. The 2008 Act as well as the original FISA statute is a grant of authority to the executive, not a criminal statute addressed to the citizenry, and yet such a grant of authority may have the effect of discouraging—or chilling—the exercise of personal liberty, in this instance the liberty to engage in private telephone conversations. Thus, even if Justice Alito's point is pursued—even if there are some offenses that are so extraordinary that we may allow the government to

119. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 6001(a), 118 Stat. 3638, 3742 (codified as amended at 50 U.S.C. § 1801(b)(1)(C) (2012)).

120. *See* Dombrowski v. Pfister, 380 U.S. 479 (1965).

121. As discussed earlier, *see supra* note 81, the Supreme Court in *Berger v. New York*, 388 U.S. 41 (1967), declared unconstitutional a New York statute establishing a process to obtain warrants allowing eavesdropping. The Court declared the statute invalid on its face and spoke of its "broad sweep," *id.* at 54, but did not formally invoke the First Amendment overbreadth doctrine.

investigate them without a warrant—the statute that permits or authorizes such investigative activity must fall when it embraces as broad a category as "foreign intelligence gathering." The legislators must go back to the drawing board and come up with a statute confined to investigations related to international terrorism. Then, but only then, will the Supreme Court have reason to decide whether international terrorism is the kind of extraordinary offense that Justice Alito contemplated and whether an investigation of such an offense justifies an abandonment of the traditional warrant requirement of the Fourth Amendment.

One branch of the principle requiring separation of powers warns against unilateral exercises of executive power. From this perspective, the 2008 statute, compared to President Bush's Terrorist Surveillance Program, might be seen as a step forward, or maybe a half-step. In it, the role of the judiciary is minimized but Congress authorized what Bush had decreed. From the perspective of the Fourth Amendment and the values it seeks to protect, however, the 2008 statute is a step backward, for its authorization of warrantless wiretapping is in no way confined to terrorism or to the investigation of any other offense that might possibly be regarded as extraordinary. Like much of what has happened during the last decade, such as the use of military commissions and prolonged, indefinite imprisonment without a trial, the 2008 measure has transformed the exception into the rule. At the moment, the authority to engage in warrantless wiretapping is confined to the process of gathering foreign intelligence, broadly construed, but if left unchecked, it will provide the foundation for a similar authority in other realms and thus become, I fear, a new point of departure.