

ELECTRONIC SURVEILLANCE OF TERRORISM IN THE UNITED STATES

*William Funk**

Over the past seventy-five years, American law relevant to government searches has distinguished between searches conducted for the purpose of gathering evidence to be used in a criminal trial and searches conducted for other purposes. Moreover, until 9/11, for both legal and practical reasons, foreign intelligence gathering (including counter-intelligence and anti-terrorism) proceeded along distinct and different tracks from law enforcement, only occasionally overlapping. Consequently, until recently, electronic surveillance for foreign intelligence purposes rarely had criminal prosecution as a goal.

Today, combating international terrorism, or the war on terror, has confused the historical distinction between intelligence gathering and law enforcement, just as it has confused the distinction between traditional criminal trials and the modes of operation applicable in recognized wars.¹ The purpose of this article is, first, to provide the history and context in which the distinction between law enforcement and intelligence searches has arisen and, second, as we go forward, to ask how we should address these issues in the future.

* Robert E. Jones Professor of Law, Lewis & Clark Law School.

¹ On April 6, 2010, the New York Times reported that the President had authorized the targeting of an American citizen for assassination. See Scott Shane, *U.S. Approves Targeted Killing of American Cleric*, N.Y. TIMES, Apr. 7, 2010, at A12, available at <http://www.nytimes.com/2010/04/07/world/middleeast/07yemen.html>. The American citizen is apparently hiding in Yemen and is believed to be involved in plots to carry out terrorist acts in the United States. Richard Reid (the shoe-bomber) was tried in a civilian court for violation of federal criminal law; Jose Padilla (the alleged dirty bomber) was initially held by the military and scheduled for trial by a military commission but ultimately was also tried in a civilian court for violation of federal criminal law. Khalid Sheikh Mohammed (the alleged 9/11 mastermind) was first to be tried in a civilian court but now appears headed for trial by a military commission, like the Nazi saboteurs in *Ex Parte Quirin*. 317 U.S. 1 (1942).

The United States has engaged in electronic surveillance for the purpose of gathering intelligence since at least the Civil War. For much of this time, the Supreme Court interpreted the Fourth Amendment's protections² against government searches to be linked to the protection against the use of evidence against a person in a criminal case.³ In other words, the government could read the Fourth Amendment not to restrict its searches for intelligence information, so long as it was not to be used as evidence in a trial. Moreover, in 1928, the Supreme Court declared that electronic surveillance (not involving trespass to install) was not even subject to the Fourth Amendment because it did not constitute a "search."⁴ There was, however, a statute applicable to wiretapping, the Communications Act of 1934,⁵ which made it a crime for any person to "intercept" and "divulge or publish" the contents of wire and radio communications,⁶ and the Supreme Court

² The text of the Fourth Amendment provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

³ See *Boyd v. United States*, 116 U.S. 616, 633 (1886) ("[T]he 'unreasonable searches and seizures' condemned in the fourth amendment are almost always made for the purpose of compelling a man to give evidence against himself, which in criminal cases is condemned in the fifth amendment; and compelling a man 'in a criminal case to be a witness against himself,' which is condemned in the fifth amendment, throws light on the question as to what is an 'unreasonable search and seizure' within the meaning of the fourth amendment."); see also *Frank v. Maryland*, 359 U.S. 360, 365-67 (1959) ("[H]istory makes plain, that it was on the issue of the right to be secure from searches for evidence to be used in criminal prosecutions or for forfeitures that the great battle for fundamental liberty was fought. . . . Inspection without a warrant, as an adjunct to a regulatory scheme for the general welfare of the community and not as a means of enforcing the criminal law, has antecedents deep in our history."), *overruled by* *Camara v. Mun. Ct.*, 387 U.S. 523 (1967).

⁴ See *Olmstead v. United States*, 277 U.S. 438, 465 (1928) ("The language of the [Fourth] amendment cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched.")

⁵ 47 U.S.C. § 605 (1964).

⁶ *Id.*

interpreted this provision to apply to the government.⁷ Nevertheless, the government read the provision according to its terms as only prohibiting interception followed by divulging or publishing the contents outside the federal establishment.⁸ In other words, the government believed it would not violate this provision by wiretapping to obtain intelligence information. Thus, the government believed that it could lawfully engage in both physical searches and electronic surveillance for intelligence purposes without being subject to the Fourth Amendment or other legal restrictions.

This state of affairs continued until 1967, when the Supreme Court decided two cases that radically changed this understanding. First, in *Camara v. Municipal Court*,⁹ the Court rejected the notion that the Fourth Amendment's protections and the requirement of a prior judicial warrant were limited to situations in which the search was for evidence to be used in a criminal prosecution, overruling its earlier decision to the contrary. Now, the Fourth Amendment's warrant requirement applied to any governmental search. Second, in *Katz v. United States*,¹⁰ the Court overruled *Olmstead* and held that electronic surveillance was a search subject to the Fourth Amendment. Thus, on their face, the cases wiped out the two basic legal justifications for searches and electronic surveillance for intelligence purposes – that they were not conducted to gather evidence for use in a criminal trial and that electronic surveillance was not subject to the Fourth Amendment. Nevertheless, *Katz* contained a footnote that the government could use to justify continued business as usual: “Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation

⁷ *Nardone v. United States*, 302 U.S. 379 (1937) (excluding evidence obtained from a wiretap); *see also* *Nardone v. United States*, 308 U.S. 338 (1939) (extending exclusion to the fruits of the surveillance).

⁸ *See* S. REP. NO. 95-604, at 10 (1977).

⁹ *Camara v. Mun. Ct.*, 387 U.S. 523 (1967) (overruling *Frank v. Maryland*, 359 U.S. 360 (1959)).

¹⁰ *Katz v. United States*, 389 U.S. 347, 359 (1967).

involving the national security is a question not presented by this case.”¹¹

This language, while not authorizing intelligence searches or surveillance without a warrant, made clear that the *Katz* decision did not require one. Moreover, given the now equivalence between electronic surveillance and physical searches, the same uncertainty would apply to physical searches for intelligence purposes. The legal limbo of national security electronic surveillance was compounded when Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968,¹² which generally criminalized electronic surveillance but specifically authorized electronic surveillance to obtain evidence for use in the prosecutions of certain crimes. However, it too contained a disclaimer, saying that nothing in the Act should be read to limit the constitutional power of the President

to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities . . . [nor] to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force . . . [or] any other clear and present danger to the structure or existence of the Government.¹³

¹¹ *Id.* at 358 n. 23. The origin of the footnote is not certain; there is no mention of national security in the government’s brief. However, the year before *Katz* the Solicitor General provided a supplemental brief in a case involving surreptitious microphone surveillance in a law enforcement case explaining that historically the FBI had used such devices

for intelligence (and not evidentiary) purposes which [were] required in the interests of internal security or national safety. . . . Present . . . practice . . . prohibits the use of such listening devices (as well as the interception of telephone and other wire communications) in all instances other than those involving the collection of intelligence affecting the national security.

S. REP. NO. 95-604, at 12 (1977). This recent revelation must have been on the Court’s mind when it decided *Katz*.

¹² Pub. L. No. 90-351, 82 Stat. 197 (1968) (codified at 18 U.S.C. §§ 2510-2520 (Supp. V 1965-1969)).

¹³ *Id.* § 2511(3).

The government's response was to institute new internal procedures, including a requirement for the personal authorization by the Attorney General under an express delegation from the President, before intelligence searches or surveillances could take place without a prior judicial warrant. The positive legal authority for the searches and surveillances would continue to be, in the absence of any positive legislatively granted authority, the inherent constitutional power of the President to obtain necessary intelligence information. The internal administrative procedures would provide the "safeguards" necessary to make the searches and surveillances reasonable.

In 1972, the Supreme Court narrowed the intelligence "exception" in *United States v. United States District Court*, known as the *Keith* case after the district court judge who was the respondent in the case.¹⁴ There the government had engaged in domestic security electronic surveillance without a warrant. It argued that:

[T]he special circumstances applicable to domestic security surveillances necessitate a further exception to the warrant requirement. . . . We are told further that these surveillances are directed primarily to the collecting and maintaining of intelligence with respect to subversive forces, and are not an attempt to gather evidence for specific criminal prosecutions. It is said that this type of surveillance should not be subject to traditional warrant requirements which were established to govern investigation of criminal activity, not ongoing intelligence gathering.¹⁵

The Court unanimously rejected the argument, holding that prior judicial warrants were necessary for domestic security surveillance, but again its opinion contained a disclaimer: "[T]his case involves only the domestic aspects of national security. We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents."¹⁶ Thus,

¹⁴ *United States v. U.S. Dist. Ct. (Keith)*, 407 U.S. 297 (1972).

¹⁵ *Id.* at 318-19.

¹⁶ *See id.* at 321-22.

government surveillance for foreign intelligence information without a warrant continued where the Attorney General found that it was directed at foreign powers or their agents.

While a number of lower courts upheld the exercise of this power if the “primary purpose” of the surveillance was to obtain foreign intelligence information,¹⁷ the claimed legal authority for warrantless surveillance for foreign intelligence remained on uncertain grounds. A plurality of the en banc D.C. Circuit had in dictum stated that a prior warrant is required even when the surveillance is directed at a foreign power or agent of a foreign power.¹⁸ Investigations by House and Senate committees had uncovered a litany of intelligence abuses, including electronic surveillance of civil rights and anti-war groups during the Vietnam War,¹⁹ resulting in bills introduced to ban intelligence surveillances altogether.²⁰ Moreover, third parties, whose help was often necessary to carry out foreign intelligence surveillances, were being sued for their complicity in the “abuses” and were reluctant to continue giving assistance.²¹ As a result, the Ford administration supported a

¹⁷ See, e.g., *United States v. Truong Dinh Hung*, 629 F.2d 908, 915 (4th Cir. 1980) (stating that “the executive should be excused from securing a warrant only when the surveillance is conducted ‘primarily’ for foreign intelligence reasons”); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977) (warrantless surveillances are “lawful for the purpose of gathering foreign intelligence”); *United States v. Butenko*, 494 F.2d 593 (3d Cir. 1974) (wiretap valid if primary purpose to gather foreign intelligence information); *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973) (upheld warrantless wiretap against U.S. citizen); *United States v. Clay*, 430 F.2d 165 (5th Cir. 1970); *United States v. Smith*, 321 F. Supp. 424, 425-26 (D. Cal. 1971).

¹⁸ *Zweibon v. Mitchell*, 516 F.2d 594, 651 (D.C. Cir. 1975).

¹⁹ See S. REP. NO. 94-755, Bk. 2, at 67-74 (1976).

²⁰ See National Security Surveillance Act of 1975, S. 743, 94th Cong. (1975); Freedom from Surveillance Act of 1974, S. 4062, 93d Cong. (1974); Surveillance Practices and Procedures Act of 1973, S. 2820, 93d Cong. (1973).

²¹ See *Foreign Intelligence Surveillance Act: Hearings Before the H. Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the Comm. on the Judiciary*, 95th Cong. 64 (1978) (statement of Hon. Morgan F. Murphy, Chairman, Subcomm. on Legis. of the H. Intelligence Comm.) (testifying that FISA legislation would make the phone company “feel much more secure” in complying with electronic surveillance requests); see also *To Amend The National Security Act of 1947 to Improve U.S. Counterintelligence Measures: Hearings on S. 2726 Before the Select Comm. on Intelligence of the United States*, 101st Cong. 116-71, 136 (1990) (testimony of Mary C. Lawton, Counsel, Office of Intelligence Policy and Review, U.S. Department of Justice) (noting the failure of the phone company to cooperate with electronic surveillance requests).

bill introduced by Senator Kennedy that would authorize electronic surveillance for foreign intelligence purposes pursuant to a special warrant requirement. This bill became the Foreign Intelligence Surveillance Act (FISA).²²

FISA, however, does not follow traditional Fourth Amendment standards for judicial warrants. For example, it does not require probable cause to believe that the person subject to the surveillance was violating a criminal law or that evidence of a crime would be disclosed by the surveillance. In addition, it distinguishes between “United States person[s]”²³ and other persons,²⁴ providing more protective standards for United States persons. Moreover, unlike a normal warrant for electronic surveillance under Title III, there is a general rule against giving notice of the surveillance to those subject to it, and the length of the surveillance can be extremely long, up to a year for one surveillance with indefinite extensions. Also unlike a normal Title III warrant for law enforcement purposes, there is no comparable requirement to minimize the acquisition of information to that specifically described in the warrant. Instead, FISA substitutes limitations on disclosure and use.

These differences from a normal warrant were justified because the government had to certify that the “purpose of the surveillance is to obtain foreign intelligence information”²⁵ Consistent with its practice before FISA, the government interpreted this language to require the primary purpose of the surveillance to be obtaining foreign intelligence information, not enforcement of the criminal laws.²⁶ Thereafter, in every

²² 50 U.S.C. § 1801 *et seq.* (1982).

²³ A “United States person” is a citizen or permanent resident alien, an organization substantially comprised of citizens or permanent resident aliens, and a corporation incorporated in the United States not subject to the control of a foreign government. 50 U.S.C. § 1801(i).

²⁴ These could include not only illegal aliens but also lawful, non-immigrant aliens, such as foreign students and workers.

²⁵ 50 U.S.C. § 1804(a)(7)(B) (1984).

²⁶ See William Funk, *Electronic Surveillance of Terrorism: The Intelligence/Law Enforcement Dilemma – A History*, 11 LEWIS & CLARK L. REV. 1099, 1123-25 (2007). See Pub. L. No. 107-56, § 218, 115 Stat. 291 (2001), where after passage of the USA PATRIOT Act, FISA changed to require merely that “a significant purpose” be to obtain

case in which FISA's constitutionality was challenged, the court upheld the constitutionality of FISA's warrant system, and in every case in which the issue was addressed, the court relied on FISA's "primary purpose" requirement.²⁷

In 1995 Congress extended FISA's special warrant system to authorize physical searches within the United States for foreign intelligence purposes.²⁸

The above discussion demonstrates the importance ascribed to the purpose of the surveillance being to obtain foreign intelligence information, rather than to obtain evidence for use in a criminal trial. Surveillances with the former purpose need not comply with traditional Fourth Amendment warrant requirements, while surveillances with the latter purpose were subject to the traditional requirements of the Fourth Amendment.

However, if a search or surveillance undertaken for a non-law enforcement purpose discloses evidence of a crime, that evidence could be used. Outside of the intelligence realm there is ample authority for the lawfulness of retaining and using, for law enforcement purposes, evidence incidentally acquired pursuant to non-law enforcement searches or surveillances.²⁹ This doctrine arises naturally from the Plain View Doctrine that allows law enforcement officers to seize evidence of crime

foreign intelligence. *See* *In re Sealed Case*, 310 F.3d 717, 721 (FISA Ct. Rev. 2002), to understand how the government changed its tune as to the original meaning.

²⁷ *See* *United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1992) (finding primary purpose required); *United States v. Pelton*, 835 F.2d 1067, 1075-76 (4th Cir. 1987) (finding a primary purpose required); *United States v. Badia*, 827 F.2d 1458, 1464 (11th Cir. 1987) (assuming a primary purpose requirement); *United States v. Duggan*, 743 F.2d 59, 77 (2d Cir. 1984) (finding primary purpose required); *United States v. Falvey*, 540 F. Supp. 1306, 1314 (N.Y. Sup. Ct. 1982) (assuming a primary purpose standard).

²⁸ *See* Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 807, 108 Stat. 3423, 3443-53 (codified as amended at 50 U.S.C. § 1822-29 (2006)).

²⁹ *See, e.g.*, *Illinois v. Lidster*, 540 U.S. 419 (2004) (roadblock search for accident investigation); *New Jersey v. T.L.O.*, 469 U.S. 325 (1985) (search of personal property to enforce school rules); *United States v. Martinez-Fuerte*, 428 U.S. 543 (1976) (border checkpoint search); *see also* *New York v. Burger*, 482 U.S. 691 (1987) (administrative search of vehicle dismantling operation); *United States v. Biswell*, 406 U.S. 311 (1972) (administrative search of firearms dealer); *Colonnade Catering Corp. v. United States*, 397 U.S. 72 (1970) (administrative search of liquor dealer).

in plain view when they otherwise are lawfully present.³⁰ Prior to FISA, all the courts considering the issue had found the doctrine applicable to electronic surveillance for foreign intelligence purposes.³¹ FISA explicitly authorized the use of incidentally acquired evidence of crimes.³²

When a search is lawful without a warrant, or pursuant to an administrative warrant so that incidentally acquired evidence may be used in a criminal prosecution, there is an incentive for the government to purport to be searching for the non-law enforcement purpose because of the lack of need to meet the stringent requirements for a traditional warrant. Courts have accordingly scrutinized whether the purported non-law enforcement purpose of the search was pretextual. If the real purpose was to obtain evidence of a crime, then a traditional warrant would be required. For example, in *Michigan v. Clifford*,³³ the Court approved the use of an administrative warrant to inspect a burned residence if the primary purpose was to determine the cause of the fire, but once the cause was determined to be arson, then the primary purpose would be to obtain evidence of the crime and a traditional warrant would be required. In the foreign intelligence field, the same rules applied. In perhaps the most famous spy prosecution to reach the Supreme Court,³⁴ Colonel Rudolf Abel of the KGB was arrested pursuant to an immigration arrest warrant for the purpose of deportation on the basis of information supplied by the FBI to the Immigration and Naturalization Service (INS) suggesting that Abel was an illegal alien. The arresting INS agents were

³⁰ See *Coolidge v. New Hampshire*, 403 U.S. 443, 465-66 (1971); see also 18 U.S.C. § 2517 (allowing the disclosure and use of evidence of a crime obtained through a lawful Title III surveillance even though not related to the purpose of the surveillance).

³¹ See *United States v. Truong Dinh Hung*, 629 F.2d 908, 915 (4th Cir. 1980); *United States v. Butenko*, 494 F.2d 593 (3rd Cir. 1974).

³² See 50 U.S.C. § 1801(h)(3) (2006).

³³ 464 U.S. 287 (1984).

³⁴ See *Abel v. United States*, 362 U.S. 217, 226 (1960); see also LOUISE BERNIKOW, ABEL. (Ballantine Books 1982) (1970) (biographical account of Abel's life, focuses on his spy work, arrest, trial, and the government's exchanging of him for U-2 pilot Gary Powers); Federal Bureau of Investigation, Famous Cases: Rudolph Ivanovich Abel (Hollow Nickel Case), <http://www.fbi.gov/libref/historic/famcases/abel/abel.htm> (overview of Abel's espionage and the FBI's pursuit thereof).

accompanied by FBI agents, and the FBI agents searched Abel's residence incident to the arrest, looking for and finding evidence of espionage. Abel challenged the lawfulness of the search, arguing that his immigration arrest was simply a ruse to enable the FBI to search his residence. The Court responded:

Were this claim justified by the record, it would indeed reveal a serious misconduct by law-enforcing officers. The deliberate use by the Government of an administrative warrant for the purpose of gathering evidence in a criminal case must meet stern resistance by the courts. The preliminary stages of a criminal prosecution must be pursued in strict obedience to the safeguards and restrictions of the Constitution and laws of the United States.³⁵

In addition, in *United States v. Truong Dinh Hung*,³⁶ what started as a surveillance for foreign intelligence purposes at a certain point became primarily a surveillance to obtain evidence of a crime. The Fourth Circuit held that at that point the surveillance was no longer lawful as foreign intelligence surveillance; it was now a law enforcement surveillance and required a Title III warrant.

So long as foreign intelligence surveillance was aimed at pure foreign intelligence, traditional counter-intelligence, or even international terrorism accomplished abroad against non-United States targets, drawing the intelligence/law enforcement line was generally not problematical, because criminal prosecution was rarely the sought-for goal.³⁷ However,

³⁵ *Abel*, 362 U.S. at 226.

³⁶ 629 F.2d 908 (4th Cir. 1980).

³⁷ Successful counterintelligence operations often, if not normally, conclude not with prosecution but some other form of neutralization, such as "doubling" an agent. For example, the FBI arrested Rudolf Abel, a Soviet agent who operated undercover for ten years in New York City, only after failing to "double" him. See *Abel*, 362 U.S. at 223; see also 140 CONG. REC. S2883-02 (1994) (per Sen. Cohen) ("Prosecution is one way, but only one way and not always the best way, to combat such activities. 'Doubling' an agent or feeding him false or useless information are other ways. Monitoring him to discover other spies, their tradecraft and equipment can be vitally useful. Prosecution, while disabling one known agent, may only mean that the foreign power replaces him with one whom it may take years to find or who may never be found."); H.R. REP. NO. 95-1283, pt. I, at 43-44 (1978) ("[I]t may be more fruitful in terms of combatting [sic] international terrorism to monitor the activities of such

the shift of international terrorism from non-United States targets abroad to domestic targets and United States targets abroad changed the nature of the problem. Now, criminal prosecution, or at least incarceration or incapacitation, was likely to be the primary goal, although the gathering of intelligence regarding the terrorists' contacts, plans, and infrastructure was also extremely important. What was the "primary" purpose even at the inception was no longer clear.

The solution, adopted in the USA PATRIOT Act in the immediate aftermath of 9/11 in light of allegations that the purpose requirement in FISA had hobbled FBI intelligence and law enforcement cooperation,³⁸ was to change FISA's requirement that the surveillance be for "the purpose" of obtaining foreign intelligence to a requirement that the surveillance merely have "a significant purpose" of obtaining foreign intelligence.³⁹ Now the primary purpose of the surveillance could be to gather evidence to use in a criminal trial even while the requirement to obtain the warrant did not require a showing of probable cause that the target was engaged in illegal activity or that evidence of a crime would be obtained. The question was then whether this solution comported with the Fourth Amendment.

The first court to consider the constitutionality of the USA PATRIOT Act amendment to FISA was the Foreign Intelligence Surveillance Court of Review (FISCR), the unusual "court of appeals" established in FISA to hear government appeals of denials of orders by the Foreign Intelligence Surveillance Court.⁴⁰ The FISCR, acknowledging that its answer was not governed by any "definitive jurisprudential answer,"⁴¹ found the amended FISA facially constitutional

persons in the United States to identify otherwise unknown terrorists here, their international support structure, and the location of their weapons or explosives.").

³⁸ See NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 78-79 (2004); see also OFFICE OF THE INSPECTOR GENERAL, A REVIEW OF THE FBI'S HANDLING OF INTELLIGENCE INFORMATION RELATED TO THE SEPTEMBER 11 ATTACKS 21-42, available at <http://www.fas.org/irp/agency/doj/oig/fbi-911/chap2.pdf>.

³⁹ See Pub. L. No. 107-056, § 218, 115 Stat. 291 (2001).

⁴⁰ See *In re Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. 2002).

⁴¹ *Id.* at 746.

despite the lack of a primary purpose to obtain foreign intelligence. The FISCRC believed the proper question to ask was whether a FISA search was “reasonable,” as required by the Fourth Amendment, not whether the authorization of surveillance granted under FISA met the constitutional standards for a search warrant. It admitted that courts had found a primary purpose test constitutionally required where there was no prior judicial warrant, but the FISCRC surmised that the additional safeguards created under FISA, beyond those that existed when foreign intelligence surveillances were conducted solely pursuant to the President’s constitutional authority, sufficed to render the authorized surveillances reasonable on their face. The court noted the many similarities between FISA and Title III surveillances, while acknowledging the significant differences in their probable cause and particularity showings. Recalling that in *Keith* the Supreme Court had stated that even domestic security surveillances might be adequately governed by procedures different from those involved in “ordinary crime,”⁴² the FISCRC concluded that the similarities outweighed the differences given the nature of surveillances relating to foreign intelligence.

While the FISCRC decision is highly defensible, it is well to remember that it was issued in an *ex parte* proceeding challenging the facial validity of the amended FISA.⁴³ Subsequently, while there have been a number of challenges to surveillances made pursuant to FISA, all but two have either ignored the change in the purpose requirement⁴⁴ or concluded that in any case the primary purpose of the surveillance was to obtain foreign intelligence.⁴⁵ The two exceptions are two

⁴² See *Keith*, 407 U.S. 297, 322 (1972) (“[W]e do not hold that the same type of standards and procedures prescribed by Title III are necessarily applicable to this case. We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of ‘ordinary crime.’”).

⁴³ The FISCRC did invite the American Civil Liberties Union and the National Association of Criminal Defense Lawyers to file briefs as *amici curiae* in the case, but this should not change the essential nature of the *ex parte* proceeding.

⁴⁴ See *United States v. Damrah*, 412 F.3d 618, 625 (6th Cir. 2005); *United States v. Benkahla*, 437 F. Supp. 2d 541, 554-55 (E.D. Va. 2006).

⁴⁵ See *United States v. Stewart*, 590 F.3d 93, 128 (2d Cir. 2009); *United States v. Islamic Am. Relief Agency*, No. 07-00087-CR-W-NKL, 2009 WL 5169536 (W.D. Mo. Dec. 21, 2009).

district court decisions, one which found FISA as amended unconstitutional because of the lack of a primary purpose requirement⁴⁶ and one which found it still constitutional.⁴⁷ Law review articles on the constitutionality of the amended FISA abound,⁴⁸ some finding it constitutional, others not. In short, the issue certainly has not been determinatively decided.

The issue here is less whether FISA as amended is constitutional according to established constitutional doctrine massaged in the inimitable American way, but rather the questions it raises about the nature of the struggle against international terrorism and the appropriate means to combat that terrorism consistent with retaining the individual freedoms citizens of developed nations have come to expect. First, we should not expect bi-partisan determinations agreed to by both political branches in an area of national security, in an apparent attempt to balance the needs of national security with individual liberties, to be likely overturned by courts on the basis of the Fourth Amendment. Here, the USA-PATRIOT Act amendment was made in the immediate aftermath of the 9/11, but it originally had a sunset provision that required it to be reconsidered in the future, under calmer conditions. It was, and the “significant purpose” change was retained. In other words, despite our general reliance on courts to protect individual liberties, history suggests that when national security is threatened from foreign aggressors, courts are likely to defer to the political branches. Here, moreover, that deference seems especially deserved, given the expression of

⁴⁶ See *Mayfield v. United States*, 504 F. Supp. 2d 1023 (D. Or. 2007), *vacated and remanded on other grounds*, 599 F.3d 964 (9th Cir. 2010).

⁴⁷ See *United States v. Abu-Jihaad*, 531 F. Supp. 2d 299, 304 (D. Conn. 2008).

⁴⁸ See, e.g., Robert C. Power, *“Intelligence” Searches and Purpose: A Significant Mismatch Between Constitutional Criminal Procedure and the Law of Intelligence-Gathering*, 30 PACE L. REV. 620 (2010); William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209 (2007); Diane Carraway Piette & Jesselyn Radack, *Piercing the “Historical Mists”: The People and Events Behind the Passage of FISA and the Creation of the “Wall,”* 17 STAN. L. & POL’Y REV. 437 (2006); David S. Kris, *The Rise and Fall of the FISA Wall*, 17 STAN. L. & POL’Y REV. 487 (2006); Viet D. Dinh & Wendy J. Keefer, *FISA and the PATRIOT Act: A Look Back and a Look Forward*, 35 GEO. L.J. ANN. REV. CRIM. PROC. iii (2006); Richard Henry Seamon & William Dylan Gardner, *The PATRIOT Act and the Wall Between Foreign Intelligence and Law Enforcement*, 28 HARV. J.L. & PUB. POL’Y 319 (2005).

concern for protecting both civil liberties and national security contained in the congressional materials.

Second, the acceptance of the “war on terror” as more than a mere sobriquet, but as a legal concept in the United States, further supports approval of “war-time” measures. Unlike the “war on drugs” or the “war on crime,” the war on terror, or at least the use of force pursuant to the Authorization for the Use of Military Force (AUMF),⁴⁹ has been accorded the status of “war” for many legal purposes.⁵⁰ Persons apprehended abroad, at least, may be treated as enemy combatants, and those alleged to have violated the laws of war (as today’s terrorists routinely do) may be prosecuted by military commission for violation of those laws, rather than prosecuted as simple criminals, although their acts may well constitute federal crimes. Whether persons apprehended in the United States, and especially United States citizens, may also be tried by military commissions as unlawful enemy combatants, as were the saboteurs in *Ex Parte Quirin*,⁵¹ is yet to be determined, although the government apparently maintains that it can.⁵² Thus, limits on surveillance that might be appropriate if the purpose were ordinary law enforcement may not be appropriate if the prosecution is to occur in military tribunals under the laws of war. At the same time, despite the claims by the government of the ability to use military tribunals, so far none have been used, and it seems unlikely that they will be used for anyone apprehended in the United States. This accords with the practice in European nations, even those that have suffered serious terrorist acts on their soil, although the “Diplock courts” in Northern Ireland were extensively used in lieu of

⁴⁹ Pub. L. No. 107-40, 115 Stat. 224 (2001).

⁵⁰ See, e.g., *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004).

⁵¹ 317 U.S. 1 (1942).

⁵² Jose Padilla, a United States citizen apprehended in the United States, was held as an enemy combatant. Challenges to that designation, asserting that he could only be criminally charged, were heard by two separate courts of appeals. One held for Padilla. See *Padilla v. Rumsfeld*, 352 F.3d 695 (2d Cir. 2003). The other held for the government. See *Padilla v. Hanft*, 423 F.3d 386 (4th Cir. 2005). The first decision, however, was reversed on other grounds. See *Rumsfeld v. Padilla*, 542 U.S. 426 (2004). The second was effectively mooted by the government transferring Padilla from military to civilian custody and trying him in a civilian court for a federal crime.

normal jury trials to try IRA activists, and at least in one case against a supporter of Al-Qaeda.⁵³

Third, perhaps FISA's limitation to intelligence regarding *international* terrorism (and foreign powers and their agents) justifies a different basis for engaging in surveillance of citizens. Allowing border searches without any suspicion and intrusive border searches on a reasonable suspicion basis, rather than probable cause, are examples of how cross-border concerns can justify searches that otherwise would not be justified. While FISA is not limited to (or even primarily aimed) at cross-border communications, the interest justifying the search technique is one that necessarily involves foreign actors or governments. Given the reduced capability of the government to obtain information abroad short of surveillance, compared to the capabilities to obtain information through less intrusive techniques in the United States, more flexibility regarding surveillance regarding such information might be justified.

These are just the beginnings of the questions that might be asked about the appropriateness, absent traditional notions of probable cause, of electronic surveillance of persons in the United States for the purpose of apprehension and prosecution. Light might be shed upon them by reference to what other developed countries with a sensitivity for individual liberties are doing in this regard. While American exceptionalism frowns on following others, here, as in other areas, such a reference might well aid in finding a suitable resolution.

⁵³ See, e.g., *Al-Qaeda Terror Suspect Convicted*, BBC NEWS, Nov. 24, 2005, available at http://news.bbc.co.uk/2/hi/uk_news/northern_ireland/4467640.stm.