Department of Homeland Security
Federal Law Enforcement Training Center
Legal Division

March 2007

The Federal Law Enforcement –Informer–

MONTHLY LEGAL RESOURCE AND COMMENTARY FOR FEDERAL LAW ENFORCEMENT OFFICERS AND AGENTS

Welcome to this installment of *The Federal Law Enforcement Informer (The Informer).* The Legal Division of the Federal Law Enforcement Training Center is dedicated to providing federal law enforcement officers with quality, useful and timely Supreme Court and Circuit Court reviews, interesting developments in the law, and legal articles written to clarify or highlight various issues. The views expressed in these articles are the opinions of the author and do not necessarily reflect the views of the Federal Law Enforcement Training Center. *The Informer* is researched and written by members of the Legal Division. All comments, suggestions, or questions regarding *The Informer* can be directed to the Editor at (912) 267-2179 or FLETC-LegalTrainingDivision@dhs.gov. You can join *The Informer* Mailing List, have *The Informer* delivered directly to you via e-mail, and view copies of the current and past editions and articles in *The Quarterly Review* and *The Informer* by visiting the Legal Division web page at: http://www.fletc.gov/legal.

This edition of *The Informer* may be cited as "3 INFORMER 07".
(The first number is the month and the last number is the year.)

Join The Informer E-mail Subscription List

It's easy! Click HERE to subscribe.

THIS IS A SECURE SERVICE. No one but the FLETC Legal Division will have access to your address, and you will receive mailings from no one except the FLETC Legal Division.

PodCasts

4th Amendment Roadmap

Hot Issues

4th AMENDMENT ROADMAP A step by step guide to searches	HOT ISSUES Supreme Court cases and emergent issues
Posted Now • **Introduction to 4th Amendment Searches** • **Who is a Government Agent?** • **Reasonable Expectation of Privacy 1 and 2** • **Probable Cause 1 and 2** • **What is a Search Warrant?** • **Search Warrant Service 1 and 2** • ***Terry* Stop and Frisk** • **Protective Sweeps** • **Search Incident to Arrest** • **Consent** **** Just Added**** • **Mobile Conveyances** • **Exigent Circumstances** • **Plain View**	**Posted Now** • **Consent Searches – *GA v. Randolph*** • **Anticipatory Warrants – *US v. Grubbs*** • **GPS Tracking** ← ****To Be Added Soon**** • **Exclusionary Rule 1 and 2** • **Inspections** • **Inventories**
Coming Soon **SELF INCRIMINATION ROADMAP** A step by step guide to **The 5th Amendment – *Miranda* – the 6th Amendment**	**Coming Soon** • **Interviewing Represented Military Suspects** • **FISA – An Overview for Officers and Agents**

Click **HERE** to download or listen

Internal Affairs Investigations Training Program

Needs Survey

The Legal Division is proposing a new training program focused specifically on internal affairs investigations. We want to build and offer a program that addresses the unique practical, procedural, and legal issues of these investigations. We need your help. Please go to the link below and complete the needs survey. Also, please let others in your agency know so that they can have an opportunity to provide input into this program.

NEEDS SURVEY

Closes April 27

*****

IN THIS ISSUE

Foreign Intelligence Surveillance Act (FISA): An Overview

Click HERE

*****

Circuit Courts of Appeals Case Summaries

Click HERE

Foreign Intelligence Surveillance Act (FISA): An Overview

James G. McAdams, III
Senior Legal Instructor
Legal Division

Introduction

The Foreign Intelligence Surveillance Act (FISA)[1] was enacted in 1978. This legislation was the Congressional response to the exposure during multiple Committee hearings of previous abuses of U.S. persons' privacy rights by certain components of the United States government. Those abuses had occurred, according to the government, as part of its efforts to counter purported threats to national security.

Unquestionably, such threats existed in and before 1978; beyond peradventure, however, they pale in comparison to the threats to national security that the United States currently faces. Those threats bear the face of terrorism, primarily foreign but domestic as well. Though FISA is not a legally usable tool for combating domestic terrorism, its electronic surveillance and physical search authority are legal and very effective methods for monitoring the activities of foreign powers and agents of foreign powers while they operate within the United States. Increasingly, indeed, overwhelmingly, the current objective of such operational activities is to thwart terrorist acts.

Terrorism, as that term is used in this writing, is the use of violent acts by an organization that is not a national government for the ultimate purpose of compelling a target government to change its policy by creating fear in the minds of the populace served by the target government.[2] More recently, the preferred form of terrorism is the suicide bomber. Perhaps the most baffling and troubling element of this form of terrorism, at least to the Western mind, is the terrorist's willingness to die. Such willingness magnifies the coercive effects of these acts because, quite simply, those acts virtually always result in greater death and destruction than other forms of force. It also provides a strong message to the targeted populace and its government of the likelihood of more pain and suffering if the target government fails to accede to the terrorist organization's demands. Finally, suicide terrorists have demonstrated that they are not deterred by traditional taboos concerning targets (e.g., children) and that they are very deft at increasing the recruitment base. Both serve to create further concerns in the targeted government about the cost of future resistance to the terrorists' demands.[3]

---

[1] 50 U.S.C. § 1801 et seq.
[2] See Alex P. Schmid and Albert J. Jongman, *Political Terrorism* (New Brunswick, NJ: Transaction Books, 1988) and the lengthy discussion in the introduction to *Patterns of Global Terrorism* (Washington: U.S. Department of State, 2001).
[3] See Robert A. Pape, *Suicide Terrorism and Democracy – What We've Learned Since 9/11* (Cato Institute, *Policy Analysis*, November 2006).

In the face of the foregoing, it is no wonder then that our Congress has recently enhanced the ability of counter terrorism agents to use FISA in the effort to discover and thereby thwart acts of terrorism aimed at our country. The following is offered as an historical context in which to view FISA as well as a summary of how FISA has evolved over the past quarter century of its existence as a tool not just to thwart terrorism but more generally as an effective means to gather foreign intelligence.

The Birth of FISA

Historically, Presidents steadfastly claimed an inherent constitutional authority to conduct warrantless electronic surveillances for non-criminal, national security purposes. This authority was grounded in the mandate found in Article II of the Constitution for the Executive to "preserve, protect and defend the Constitution of the United States." This position was accorded great judicial and congressional deference for many years, but that began to change in the early 1970's.

In 1972, the Supreme Court decided the case of United States v. United States District Court, better known as the "Keith" case, in which the Court considered the legality of an Attorney General authorized warrantless electronic surveillance of a U.S. citizen accused of bombing a CIA building. The Court rebuffed the government's entreaty to recognize a foreign intelligence exception to the *per se* warrant requirement, holding that the Fourth Amendment prohibited warrantless surveillance directed at domestic threats to U.S. national security. The Court expressly refused, however, to decide the legality of warrantless surveillances where "foreign powers or their agents" were involved, leaving open the issue of the Executive's authority to direct such operational activities at those persons or entities. The Court also strongly urged the Congress to provide a judicially-manageable standard applicable to electronic surveillances conducted for national security purposes.

The Executive's use of electronic eavesdropping was again thrust into the public and congressional eye during the Watergate scandal. Revelations during several Senate Committee hearings[4] detailed warrantless privacy infringements, both by electronic surveillance and physical search, of U.S. citizens, including a U.S. congressman, some congressional staffers, anti-war protesters, and the late Martin Luther King, Jr. The Church Committee, in its final report, characterized the state of the law in this area as "riddled with gaps and exceptions", and echoed the call of the "Keith" court for Congress to create appropriate guidelines for the exercise of foreign intelligence surveillances.

Congress soon responded. In 1978, it presented the Foreign Intelligence Surveillance Act to President Carter, who signed it into law. That law established, first, that non-criminal electronic surveillances within the United States were only permissible for the purpose of

[4] These hearings were conducted under the leadership of then Senator Frank Church of Idaho, and they later became known as the "Church Committee" hearings. The committee's final report, delivered on April 26, 1976, detailed the lawlessness of U.S. intelligence agencies and the need for Congress to assert itself to stop that lawlessness through the Constitutional system of checks and balances on Executive powers. See *Frank Church and the Abyss of Warrantless Wiretapping*, by John Nichols, *The Nation*, April 26, 2006.

collecting foreign intelligence and/or foreign counterintelligence. Second, it identified foreign powers and agents of foreign powers as the entities and persons that could be targeted for electronic surveillance. Third, it articulated a probable cause standard that had to be met before an electronic surveillance was permissible. Fourth, the Act established the Foreign Intelligence Surveillance Courts (FISC), one at the district court level for initial review of surveillance applications, and one at the appellate level should the government appeal a district level denial of an application. Finally, the Act established the only circumstances under which an electronic surveillance could lawfully be conducted in the United States for the purpose of collecting foreign intelligence or foreign counterintelligence:

(1) pursuant to an order issued by the FISC; or
(2) in emergency circumstances, pursuant to Attorney General approval, so long as an application is thereafter made to the FISC within 24 hours.

FISA identifies two categories of potential targets for surveillance under FISA. The first category is foreign powers. A foreign power is –

(1) a foreign government,
(2) a diplomat, other representative or employee of a foreign government,
(3) a faction of a foreign nation that is not substantially composed of U.S. persons,
(4) an entity openly acknowledged by a foreign government to be directed and controlled by it, or
(5) a group engaged in international terrorism or activities in preparation therefore.

A second category of FISA targets are agents of foreign powers. An agent of a foreign power is –

(1) anyone, other than a U.S. person, who acts in the United States as an officer or employee of a foreign power, or
(2) anyone who acts as part of or in support of a foreign power's efforts to engage in clandestine intelligence gathering activities in the U.S.

An agent of a foreign power is also anyone, including a U.S. person, who –

(1) knowingly engages in clandestine intelligence gathering activities for a foreign power which activities constitute a violation of U.S. criminal statutes;
(2) knowingly engages in sabotage or international terrorism, or activities in reparation therefore, on behalf of a foreign power.

For purposes of the Act, a U.S. person is defined as any of the following:

(1) a citizen of the U.S.;
(2) an alien lawfully admitted for permanent residence;
(3) an unincorporated association a substantial number of which are U.S. citizens or aliens lawfully admitted for permanent residence; or
(4) a U.S. corporation.

Under the Act, international terrorism is defined as:

(1) activities that involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the U.S. or of any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;
(2) acts that appear to be intended to intimidate or coerce a civilian population, to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by assassination or kidnapping; and
(3) activities that occur totally outside the U.S., or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

Expansion of FISA Authority

1. Physical Searches

In 1995, FISA was expanded by Congress to include physical searches as well as electronic surveillance.[5] That authority permits the FISC, upon the requisite probable cause showings, to enter an order permitting the physical search of certain premises upon a probable cause showing that

(1) the target of such search is a foreign power or an agent of a foreign power;
(2) the premises to be searched contains foreign intelligence information; and
(3) the premises to be searched is owned, used, possessed by, or is in transit to or from a foreign power or agent of a foreign power.

The new physical search provisions also recognized the President's limited authority to authorize physical searches to acquire foreign intelligence without a court order. Specifically, acting through the Attorney General, the President may authorize for periods up to one year the search of any premises if the Attorney General certifies to the FISC that the premises or property to be searched is being used or controlled exclusively by a foreign power, and that there is no substantial likelihood that the search will involve the premises, information, material, or property of a U.S. person.

2. Pen Registers/Trap and Trace Devices

In 1998, Congress further amended FISA to permit the installation and use of pen register and trap and trace devices in the investigation of international terrorism and clandestine intelligence activities.[6] Applications for the installation and use of such devices must be made by the Attorney General or a designated attorney for the government and must include the applicant's certification that the information likely to be produced through the use is relevant to

[5] 50 U.S.C. §§ 1821-1829.
[6] 50 U.S.C. §§ 1841-1846.

an ongoing investigation to protect against international terrorism or clandestine intelligence activities. This new authority extends not only to the tracking of telephone calls but also to the tracking of any form of electronic communication, such as e-mails. The new section includes an admonishment, however, that specifically prohibits the investigation of U.S. persons for activities that are protected by the first amendment to the U.S. Constitution.

FISA and Law Enforcement

Some may ask, with ample justification, what possible relevance could any of the foregoing have to a law enforcement officer, federal or otherwise. The simple answer is that FISA wire taps and searches often result in the acquisition of evidence of a crime.

A case in point is the "Brothers to the Rescue" (BTTR) case that was prosecuted a few years ago by the United States Attorney's Office in the Southern District of Florida. BTTR was a group of Cuban expatriates and sympathizers in Miami who, among other things, ran air and sea patrols in the Straits of Florida to assist Cuban rafters attempting to escape Communist Cuba to make it safely to Florida. Under U.S. policy then, and now, Cubans who are successful in making landfall in Florida are paroled into the country while those interdicted before reaching Florida are repatriated to Cuba. In the BTTR case, a plane being operated by that group in international air space was shot down by a Cuban Mig. This occurred at a time when the U.S. government had identified several individuals living and working in Miami who were Cuban agents actively engaged in spying on Miami Cubans who were active in the anti-Castro movement in that city. In light of their status as agents of a foreign power, Cuba, the U.S. counter-intelligence community had several FISA wiretaps directed at them. As the result, the U.S. acquired some potentially useful evidence that would be relevant to the prosecution of the Cuban agents. When a FISA wiretap or search reveals evidence of a crime, the FBI is obligated under both Executive Order 12333[7] and the terms of the Foreign Intelligence Surveillance Act, to take reasonable steps to pass such evidence to the law enforcement community for use in investigating and/or prosecuting that case as a criminal matter.

1. The "Wall"

There is, however, a host of issues attendant to that process. One of considerable significance, with which many in the law enforcement and foreign counterintelligence (FCI) communities have struggled for many years, is this: under what circumstances may a FCI investigation in which a FISA wiretap is used be maintained when the most dramatic and practical use of the information obtained from the wire is evidence of a crime.

Since virtually immediately after its being signed into law, the majority of the FCI and foreign intelligence (FI) communities viewed FISA as being subject to the requirement that the primary purpose behind the use of wiretaps or searches executed under its authority be for the acquisition of FCI or FI. Conversely, the belief was that FISA could not be used as an investigative tool if the primary purpose of the investigation was, for example, the criminal prosecution of the target, even if the criminal prosecution would be for the crime of espionage.

[7] E.O. 12333, Sec. 2.6. President Reagan signed EO 12333 on December 4, 1981. Its complete text appears at 46 FR 59941, 3 CFR, 1981 Comp., p. 2.

Indeed, the constitutionality of FISA was challenged under either or both of the Fourth and Fifth Amendments in several cases in which information acquired through a FISA electronic surveillance was used in a subsequent criminal prosecution. The courts rebuffed those challenges, however, because the government was able to demonstrate that, throughout the FISA surveillances, the purpose thereof had been to secure foreign intelligence information rather than being primarily oriented towards assisting a criminal investigation or prosecution.[8] Nevertheless, these cases served as the genesis of the so-called "primary purpose" test and as the catalyst for the view that foreign intelligence investigations and criminal investigations had to be kept separate from each other.

During the years following these challenges, the Department of Justice (DOJ) and the intelligence community developed a practice in support of the "primary purpose" test aimed at foreclosing the perception that FISA authority was used primarily towards assisting a criminal investigation or to circumvent the more strenuous requirements imposed by federal criminal law[9] in order to obtain a wiretap order in a criminal investigation. That practice eventually became policy, a policy that was reduced to writing by DOJ in 1995, and was commonly referenced as "the wall." Indeed, the "wall" crept into the minimization and application procedures approved by the Attorney General for FISA intercepts such that by late 1995 all FISA applications contained sufficient information to justify the FISC's finding that the "primary purpose" of any particular electronic intercept would be the acquisition of foreign intelligence.

An inescapable consequence of "the wall" was the inhibition of the sharing of information between the intelligence and law enforcement communities. In the 1990's and into the early 2000's, the two communities attempted to resolve their differences and concerns over this policy with the express purpose of improving information sharing between the two communities. While serving to highlight the difficulties of changing long-ingrained cultures, those efforts were largely unsuccessful, however.

2. The USA PATRIOT Act

That reticence notably lessened following the events of September 11, 2001, and the October 2001 enactment of the United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, or the USA PATRIOT Act.[10] The Act consists of ten separate Titles and 156 sections, and which effected modifications of numerous existing federal statutes and rules. In passing the Act, the President and Congress articulated four primary purposes:

(1) Enhancing the federal government's capacity to share intelligence,
(2) Strengthening the criminal laws against terrorism,
(3) Removing obstacles to investigating terrorism, and

---

8 See, e.g., *United States v. Troung Dinh Hung*, 629 F.2d 908 (4th Cir. 1980); *United States v. Pelton*, 835 F.2d 1067, 1074-76 (4th Cir. 1987), *cert. denied*, 486 U.S. 1010 (1988)(electronic surveillance under FISA is constitutional if primary purpose of surveillance throughout surveillance was gathering of foreign intelligence; primary purpose is not changed merely because government anticipates using fruits of FISA surveillance in criminal prosecution).

9 The Omnibus Crime Control Act of 1968, also known as "Title III," at 18 U.S.C. § 2510 et seq.

10 P.L. 107-56 (October 27, 2001).

(4) Updating the law to reflect new technology.

In pursuit of those objectives, the Act, among other things, amended the requirement that the applicant for a FISA order certify that ***the purpose*** of the surveillance is to obtain foreign intelligence to require only that the applicant certify that ***a significant purpose*** of the surveillance is to obtain foreign intelligence.[11]

3. The "Wall" Falls

In May 2002, the Office of Intelligence Policy and Review (OIPR), the component of the Department of Justice (DOJ) that oversees electronic surveillance and search warrant applications submitted to the Foreign Intelligence Surveillance Court (FISC), sought to have that Court vacate the minimization and "wall" procedures as to international terrorism cases that had then been in place for some seven years. To be sure, much of the driving force behind that effort was from the events of 9/11 and the objective of eliminating real and perceived impediments to information sharing between the intelligence and law enforcement communities.

In particular, the government sought approval to allow criminal prosecutors "to advise FBI intelligence officials concerning 'the initiation, operation, continuation, or expansion of FISA searches or surveillance.'" [12] The FISC interpreted such request to be to obtain the Court's blessing of the use of FISA "primarily for a law enforcement purpose."[13]

The FISC granted a portion of DOJ's motion but explicitly declined to remove the "wall" protecting raw FISA materials from access by the criminal sections of the DOJ and FBI. Explaining its reasoning, the FISC said its objective was to prevent the law enforcement officers from becoming "de facto partners in FISA surveillances and searches" while permitting extensive sharing of information between such investigations.[14]

> Advising FBI intelligence officials on the initiation, operation, continuation or expansion of FISA surveillances and searches of U.S. persons means that criminal prosecutors will tell the FBI when to use FISA (perhaps when they lack probable cause for a title III electronic surveillance), what techniques to use, what information to look for, what information to keep as evidence and when use of FISA can cease because there is enough evidence to arrest and prosecute. The 2002 minimization procedures give the Department's criminal prosecutors every legal advantage conceived by Congress to be used by U.S. intelligence agencies to collect foreign intelligence information,… based on a standard that the U.S. person is only using or about to use the places to be surveilled or searched, without any notice to the target unless arrested and prosecuted, and, if prosecuted, no adversarial discovery of the FISA applications and warrants. All of this may

---

11 50 U.S.C. § 1804(a)(7)(B).

12 In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 623 (U.S. Foreign Intell. Surveil. Ct. 2002).

13 *Id.* at 623.

14 *Id.* at 620. The Court went on to explain that a significant part of its concern over lowering the wall was the significant number of past instances where FISA applications had included false, inaccurate or misleading information regarding information sharing or compliance with "wall" procedures by the FBI.

> be done by use of procedures intended to minimize collection of U.S. person information, consistent with the need of the United States to obtain and produce foreign intelligence information. If direction of counterintelligence cases involving the use of highly intrusive FISA surveillances and searches by criminal prosecutors is necessary to obtain and produce foreign intelligence information, it is yet to be explained to the Court.[15]

The FISC concluded its review by substituting its own minimization standards for some of those proposed by the Attorney General. Those provisions allowed the counterintelligence components of DOJ and the FBI to work in a coordinated manner with their criminal component counterparts to protect against hostile acts and clandestine intelligence activities by foreign powers. On the other hand, the Court's substitute language prohibited action by the counterintelligence component at the recommendation or request of the criminal component to initiate, operate, continue, or expand FISA surveillances or searches. In addition, the Court directly foreclosed the use of FISA procedures to enhance criminal prosecutions.[16] DOJ did not appeal the FISC's memorandum opinion and order. Rather, it awaited the FISC's application of the new minimization standards and the imposition, consistent therewith, of restrictions on the government's use and sharing of FISA information. That occurred during the summer of 2002 when DOJ sought the FISC's approval for a renewal of electronic surveillance authority in a particular case. DOJ's application sought to have the Court impose the Attorney General's new minimization standards; consistent with its earlier memorandum opinion, however, the FISC rejected DOJ's request and retained the more-restrictive earlier minimization standards. DOJ appealed that order to the U.S. Foreign Intelligence Surveillance Court of Review. This appeal constituted the first time ever that this Court had been called to meet.

The Court of Review issued a *per curiam* opinion on November 18, 2002.[17] In that opinion, the Court of Review reversed the FISC's order and remanded the case to the FISC for further proceedings consistent with the Court of Review's opinion. Though DOJ was not appealing the FISC's May 2002 decision and thus that decision was not before the Court of Review, the latter Court made it clear in its opinion that the lower court's earlier decision was, in fact, what the government was challenging.[18]

The Court of Review noted that DOJ had raised several arguments. First, the FISC's conclusion that FISA could only be used where the government's primary purpose in doing so was the acquisition of foreign intelligence found no support either in the statute or in its underlying legislative history. Second, even if the primary purpose requirement was based in the statute, the USA Patriot Act eliminated that requirement and, thus, the FISC's order amounted to "an end run" around the USA Patriot Act. Third, the minimization procedures imposed by the FISC constituted a constitutionally impermissible intrusion into DOJ's executive authority. Finally, the Fourth Amendment did not require that the primary purpose test be met in order to

---

15 *Id.* at 624. The FISC expressly declined to reach the question of whether FISA may be used primarily for law enforcement purposes. Rather, its focus was upon what minimization procedures should be approved. *Id.* at 615 n.2.
16 *Id.* at 625.
17 In re Sealed Case, 310 F.3d 717 (U.S. Foreign Intell. Surveil. Ct. Rev. 2002).
18 *Id.* at 721.

engage in the operational activities otherwise allowed under FISA.[19] The Court of Review concluded that the FISC had erred in that it misconstrued its authority under FISA. More particularly, the Court noted no authority within FISA for the FISC's reliance on the "minimization procedures" that FISA requires as a basis "to limit criminal prosecutors' ability to advise FBI intelligence officials on the initiation, operation, continuation, or expansion of FISA surveillances to obtain foreign intelligence information, even if such information includes evidence of foreign intelligence crime."[20] The Court of Review also found that the FISC had erred in refusing to consider the significance of the Patriot Act's amendments to FISA. In particular, the Court stated that, while the statute, as amended, only required certification by DOJ that " a significant purpose" of a given FISA surveillance or search be to gather foreign intelligence, the FISC's order, in effect, retained the earlier threshold, that is, that "the purpose" of the operational activity must the to gather foreign intelligence. This, the Court found, ran contrary to Congress' intent, evidenced by Members' statements during floor debates about amending the Act, to reduce existing barriers between law enforcement and foreign intelligence gathering where the target of proposed surveillance is both a potential source of valuable intelligence and the potential target of a criminal prosecution.[21] Indeed, the Court stated that, given Congress' explicit authorization of consultation and coordination between criminal and foreign intelligence components within the government concerning particular instances of the use of FISA, it necessarily follows that either of those two components may take the lead in the conduct of the underlying investigation "[s]o long as the government entertains a realistic option of dealing with the agent [of the foreign power] other than through criminal prosecution.[22] The Court of Review added, however, that its opinion must not be construed to allow the use of FISA to investigate ordinary crimes that are not intertwined with foreign intelligence crimes.[23]

Thus, "the Wall" tumbled into a grave well dug for it by the Court of Review. Future criminal defendants predictably will mount de facto "wall"-based challenges of FISA-collected evidence in their cases, citing the intelligence purpose behind that collection was only "significant" or that law enforcement was attempting to circumvent the Fourth Amendment. Otherwise, however, it seems that we have mercifully seen the last of it.

Disclosure and Use of FISA Information

Disclosure by a federal officer or employee of information acquired pursuant to one of the provisions of FISA must be for a lawful purpose and is only permitted where the disclosure is accompanied by an admonishment that use of FISA information or FISA-derived information in a criminal proceeding may only occur with advance authorization of the Attorney General. When such use is intended, the government, before the trial or other proceeding at which disclosure is to be made, must give notice of its intent to the aggrieved person and to the Court.[24] An aggrieved person may thereafter move to suppress the FISA-related evidence based on either

---

19 *Id.* at 722 & n.6.
20 *Id.* at 731.
21 *Id.* at 732-33. See also, 147 Cong. Rec. S10992 (Oct. 25, 2001), S10591 (Oct. 11, 2001), and S 11021 (Oct. 25, 2001).
22 *Id.* at 734-35.
23 *Id.* at 736.
24 50 U.S.C. §§ 1801(k), 1825(d), and 1841(3) provide definitions of "aggrieved person." Essentially, it means any person whose conversation, property, or electronic data has been intercepted pursuant to the authority of the FISC.

the argument that the FISA information was unlawfully acquired, or that the government the government in some way acted outside of the FISC order. If the court grants that motion, the government must either appeal or refrain from using any evidence that is subject to the court's order. Denial of the motion by the court will allow the government to use the FISA evidence.

Under FISA as it existed prior to the enactment of the USA Patriot Act, the FBI Director or his designee was authorized to apply for an order from the FISC requiring the production of business records held by a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility to release records in its possession where such records were relevant to an ongoing investigation to gather foreign intelligence or concerning international terrorism. As amended by the USA PATRIOT ACT, FISA authority to access business records was substantially broadened and now may, with FISC approval, compel production of "any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.[25]

It is important to re-emphasize one of the requirements of FISA that was not changed by the USA PATRIOT Act: the Attorney General must approve in advance any public disclosure of FISA materials, including the use of such materials as evidence in a criminal case - no exceptions. Even with the Attorney General's approval of the use of FISA-obtained evidence, the FBI will remain adamant that it not be required to show a FISA application to defense counsel. In the 21 years since FISA was enacted, the government has never publicly divulge a FISA application. In order to ensure that a FISA wire tap was lawful, the application is submitted ex parte, en camera to the judge in the criminal case in which the FISA take will be offered. If the judge is satisfied that the FISA application is sufficiently comprehensive for him to decide its legal adequacy, he will enter his ruling without disclosure of the application itself to the defense. If the trial judge is not so satisfied, the statute then requires disclosure of the application only if the government nevertheless intends to proceed. That, however, has never happened.

Conclusion

FISA has since its enactment been a bold and productive tool in this country's fight against the efforts of foreign governments and their agents to engage in intelligence-gathering aimed at the U.S. government, either to ascertain its future policy or to effect its current policy, to acquire proprietary information not publicly available, or to engage in disinformation efforts. With the enactment of the USA PATRIOT Act FISA has been expanded and broadened to make it a useful tool in exposing and combating foreign terrorist groups' efforts to target the United States. In recognition that such acts cannot be neatly or easily separated into intelligence versus criminal cases, the FISA Court of Review has clarified the threshold that must be met in order for FISA to be used. The Court eliminated the "primary purpose" doctrine, under which no FISA-related operational undertaking could occur unless it was primarily intended to obtain foreign intelligence. Rather, the Court, relying on its understanding of the Congressional intent behind the enactment of FISA and the wording of FISA itself, held that a FISA-related operation

[25] 50 U.S.C. § 1861(a)(1).

is justified where "a significant purpose" of such operation is to obtain foreign intelligence. This has cleared away much of the detritus that developed around FISA that had historically impeded the use of FISA in criminal investigations and the use of FISA information in criminal prosecutions.

Jim retired from the DoJ in 2006 after a 25 year career with the United States Attorney's Office in the Southern District of Florida. During that time, he served as an AUSA, the Chief of the Narcotics Division, Executive AUSA, Acting USA, Managing AUSA of the West Palm Beach Branch Office, and Senior Litigation Counsel. In 1994 Attorney General Janet Reno appointed Jim to be co-chair of a Joint Intelligence Community and Law Enforcement Working Group. In June 1995 Attorney General Reno appointed Jim as her Counsel for Intelligence Policy. In that position, he served as liaison with the various components of the Intelligence Community and also oversaw all submissions of wiretap and physical search applications by the FBI and NSA to the Foreign Intelligence Surveillance Court. Jim joined the Legal Division staff as a Senior Instructor in 2006.

*****

CIRCUIT COURTS OF APPEALS
CASE SUMMARIES

4th CIRCUIT

***US v. Kimbrough*,** 2007 U.S. App. LEXIS 3488, February 16, 2007

Showing arrestee's mother evidence found in her home, allowing her, on her own initiative, to speak with her son while remaining in their presence is not the "functional equivalent of questioning." Absent evidence of an express or tacit agreement, discussion, or understanding between the police and the mother that she would ask questions or attempt to elicit incriminating information, *Miranda* warnings are not required.

Click **HERE** for the court's opinion.

* * * *

5th CIRCUIT

US v. Gomez-Moreno, 2007 U.S. App. LEXIS 3251, February 12, 2007

Exigent circumstances may not consist of the likely consequences of the government's own actions or inactions. In determining whether officers create an exigency, this Court focuses on the "reasonableness of the officers' investigative tactics leading up to the warrantless entry."

A "knock and talk" strategy is reasonable where the officers who approached the house are not convinced that criminal activity is taking place or have any reason to believe the

occupants are armed.

Creating a show of force and demanding entry into a home without a warrant, goes beyond the reasonable "knock and talk" strategy of investigation and unreasonably creates the exigency.

Click **HERE** for the court's opinion.

* * * *

US v. Meredith, 2007 U.S. App. LEXIS 4235, February 26, 2007

After ordering an occupant to exit a vehicle and hearing that he claims to be physically unable to do so, an officer may open the occupant's door and conduct a minimally necessary visual inspection of the person of that occupant. Further, if this inspection reveals articulable facts constituting reasonable suspicion that the occupant is armed and dangerous, he may be patted down to the same extent as he could have been if he had complied with the order to exit the vehicle. Officers need no suspicion to order the occupants to step out of the car. Likewise, officers need no suspicion to open the door and perform a brief visual check of the disabled occupant.

Click **HERE** for the court's opinion.

* * * *

6th CIRCUIT

US v. Stover, 474 F.3d 904, January 30, 2007

Officers with an arrest warrant and reason to believe that the suspect is inside the house may enter and search anywhere that the suspect might reasonably be found. Once a suspect is found, the arrest warrant does not justify a more intrusive search of the premises. Generally, the government may not search an individual's home without the individual's consent or a search warrant. A limited exception to this general rule authorizes officers making arrests in the home to conduct a "protective sweep"–a quick and limited search of the premises, incident to an arrest and conducted to protect the safety of the police officers and others. The fact that police identified a car registered to a local criminal who did not live at defendant's address is sufficient to justify a quick and limited protective sweep. Even though defendant lived in a duplex, the criminal who owned the car in defendant's driveway was as likely to be visiting defendant as he was to be visiting defendant's neighbor. This probability is sufficient to justify a protective sweep.

Click **HERE** for the court's opinion.

* * * *

Livermore v. Lubelan, 2007 U.S. App. LEXIS 2594, February 7, 2007

In the excessive force context, it is not enough that a plaintiff establishes that the defendant's use of force was excessive under the Fourth Amendment. To defeat qualified immunity, the plaintiff must show that the defendant had notice that the manner in which the force was used had been previously proscribed.

The ultimate inquiry is "whether the totality of the circumstances justifies a particular sort of seizure." Three factors (not an exhaustive list) are considered in determining the reasonableness of force used: (1) the severity of the crime at issue; (2) whether the suspect posed an immediate threat to the safety of the police officers or others; and (3) whether the suspect actively resisted arrest or attempted to evade arrest by flight.

Even when the particular seizure is reasonable, liability exists if the defendant police officers acted recklessly in creating the circumstances which required the use of deadly force.

Click **HERE** for the court's opinion.

* * * *

US v. Rice, 2007 U.S. App. LEXIS 4778, March 2, 2007

Title III requires that an application for a wiretap order contain full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous. This is referred to as the "necessity requirement," the purpose of which is to ensure that a wiretap is not resorted to in situations where traditional investigative techniques would suffice and to protect against the impermissible use of a wiretap as the initial step in a criminal investigation. A purely conclusory affidavit unrelated to the instant case and not showing any factual relations to the circumstances at hand is inadequate compliance with the statute.

The "good faith" exception of *United States v. Leon*, 468 U.S. 897 (1984), does not apply to warrants improperly issued under Title III.

Click **HERE** for the court's opinion.

* * * *

7th CIRCUIT

US v. Renken, 474 F.3d 984, January 31, 2007

Consent to search can be voluntary even when given while a defendant is in custody without having received *Miranda* warnings. Custody alone has never been enough in itself to demonstrate a coerced confession or consent to search.

Under *United States v. Patane*, 124 S. Ct. 2620, 2629 (2004), the failure to give *Miranda* warnings does not require the exclusion of real evidence collected after a defendant gives a voluntary consent to search. Instead, the "totality of the circumstances" analysis applies.

Click **HERE** for the court's opinion.

* * * *

US v. Garcia, 474 F.3d 994, February 2, 2007

Looking at this issue for the first time, the Court decides:

Placing a GPS (global positioning system) "memory tracking unit" underneath the rear bumper of a car found in a public place is not a Fourth Amendment "seizure" because the device did not affect the car's driving qualities, did not draw power from the car's engine or battery, did not take up room that might otherwise have been occupied by passengers or packages, and did not alter the car's appearance.

Using the device to track the car in public is not a Fourth Amendment "search" requiring probable cause and a warrant.

The courts of appeals have divided over the question.

The 5th and 9th circuits agree, although the 5th circuit approved of but did not expressly require a showing of reasonable suspicion. (cites omitted).

The 1st, 6th, and 10th circuits call tracking a "search." The 1st and 6th circuits require probable cause but no warrant. (cites omitted).

Click **HERE** for the court's opinion.

Click **HERE** for an article on GPS tracking by FLETC LGD Senior Instructor Keith Hodges(written prior to this decision).

* * * *

US v. Horne, 474 F.3d 1004, February 5, 2007

The Hobbs Act, 18 U.S.C. § 1951(a) makes robbery that "in any way or degree obstructs, delays, or affects commerce" a federal crime.

eBay, the online auction site, is an avenue of interstate commerce, like an interstate highway or long-distance telephone service. The use of eBay to lure a victim is use of an interstate instrumentality for purposes of the Hobbs Act.

Click **HERE** for the court's opinion.

US v. Wiley, 475 F.3d 908, February 6, 2007

When an affidavit is based on informant tips, the probable cause inquiry is based on the totality of the circumstances. *See Illinois v. Gates*, 462 U.S. 213 (1983). These four factors are particularly relevant as a part of this inquiry: (1) the extent to which the police have corroborated the informant's statements; (2) the degree to which the informant has acquired knowledge of the events through firsthand observation; (3) the amount of detail provided; and (4) the interval between the date of the events and police officer's application for the search warrant.

Probable cause does not require direct evidence linking a crime to a particular place. Issuing judges are entitled to draw reasonable inferences about where evidence is likely to be found given the nature of the evidence and the type of offense. In the case of drug dealers, evidence is often found at their residences. However, there is no categorical rule that would, in every case, uphold a finding of probable cause to search a particular location simply because a suspected drug trafficker resides there.

Click **HERE** for the court's opinion.

* * * *

8th CIRCUIT

US v. Williams, 2007 U.S. App. LEXIS 3248, February 13, 2007

An affidavit is not robbed of its probative effect by its failure to mention that the informant "was a paid informant who avoided prosecution by virtue of her testimony…." In fact, a properly developed pay-based incentive system with appropriate consequences for invalid information may even bolster reliability. Omitting the details and existence of the bargaining agreement between the informant and the government is not misleading.

Probable cause is not defeated by a failure to inform the magistrate judge of an informant's criminal history if the informant's information is at least partly corroborated or reliability is established through some other means such as a track record.

Click **HERE** for the court's opinion.

* * * *

10th CIRCUIT

US v. Walker, 474 F.3d 1249, January 31, 2007

Opening the storm door to knock on the inner door, even though the inner door was partially open, is not a Fourth Amendment intrusion because such action does not violate an occupant's reasonable expectation of privacy.

When the Deputy knocked on the inner door, again announcing that he was from the Sheriff's office, defendant responded, "Yeah, and I got a goddamn gun." This threatening remark justified the officers in taking prompt action to protect themselves. Although retreat was an alternative, it was also reasonable for them to take control of the situation by entering to disarm Mr. Walker, who could otherwise continue to pose a danger to the officers and others.

A "protective sweep" is a quick and limited search of premises, incident to an arrest and conducted to protect the safety of police officers or others. Absent an arrest warrant or even probable cause to make an arrest, a protective sweep is not authorized.

Editor's Note: The court remanded the case to the district court to determine whether the "sweep" was lawful under the emergency exigency. If so, the evidence found during the "sweep" that justified the eventual arrest was seized under the "plain view doctrine" and would therefore be admissible.

Click **HERE** for the court's opinion.

* * * *

US v. Brakeman, 475 F.3d 1206, February 6, 2007

An officer's personal knowledge cannot be the *sole* means of determining what property is to be searched but it can supplement a technically inaccurate description in a search warrant to cure any ambiguity and satisfy the Fourth Amendment's particularity requirement.

Click **HERE** for the court's opinion.