

CONFIDENTIAL INFORMANTS IN NATIONAL SECURITY INVESTIGATIONS

Abstract: Although a body of law has developed around the use of confidential informants in criminal investigations, the role of informants in national security matters is less clearly defined. This Note first examines the limitations on the use of informants in the criminal context that are imposed by the Fourth Amendment, a detailed set of guidelines issued by the Attorney General, and other sources of law. It then turns to the treatment of informants by the major sources of national security law, including the Foreign Intelligence Surveillance Act. Ultimately, this Note concludes that in the national security context, government agents are free from many of the restrictions placed on the use of informants in criminal investigations. Although this relative freedom may be necessary given the immediate challenge of combating international terrorism, care should be taken that the executive branch does not use informants in a way that violates individual privacy or oversteps other proper investigative boundaries.

INTRODUCTION

Informants, otherwise known as “snitches” or “rats,” are people who report to the authorities on the criminal activity of others.¹ Informants may be one-time providers of information or recurring agents of law enforcement.² By nature, many informants are criminals themselves, and, as a result, law enforcement agents in the United States often rely on criminals to help solve and prevent crimes.³ As a practical reality, informants are a necessary evil in criminal investigations, but employing underworld figures as allies may create legal and ethi-

¹ See ROBERT M. BLOOM, *RATTING: THE USE AND ABUSE OF INFORMANTS IN THE AMERICAN JUSTICE SYSTEM* 1-7 (2002) (introducing the role of informants throughout history); DICK LEHR & GERARD O'NEILL, *BLACK MASS: THE IRISH MOB, THE FBI, AND A DEVIL'S DEAL*, at xiii (2000) (referring to informants as “snitch[es]” and “rats”).

² BLOOM, *supra* note 1, at 1.

³ See *id.* at 1-7.

cal concerns.⁴ Therefore, a body of law has developed around the use of informants in criminal investigations.⁵

The nation's law-enforcement agencies now face a major new challenge: preventing another terrorist attack inside the United States.⁶ As some reports suggest, the Federal Bureau of Investigation (the "FBI") and other agencies have engaged informants with links to terrorist organizations in order to detect and prevent future terrorist plots.⁷ In national security investigations, however, the policies regarding informants differ from those in the criminal context.⁸ This Note addresses how the rules governing the use of informants change when national security is at stake.

The law imposes a number of restrictions on the use of informants in criminal investigations. Under the Fourth Amendment, courts may issue search warrants on the basis of information provided by an informant, but only upon a preliminary demonstration that the source of such information is somewhat reliable.⁹ An even more stringent standard of review is imposed upon the use of informants to support an application for electronic surveillance.¹⁰ In addition to these warrant requirements, other defenses and remedies exist for the criminally accused whose rights may have been violated during an investigation involving the use of informants.¹¹ Furthermore, the Attorney General has issued detailed guidelines regulating the manner in

⁴ For a discussion of the legal and ethical problems attending the use of informants in the criminal context, see *infra* notes 28–104 and accompanying text.

⁵ See Amanda J. Schreiber, Note, *Dealing with the Devil: An Examination of the FBI's Troubled Relationship with Its Confidential Informants*, 34 COLUM. J.L. & SOC. PROBS. 301, 340–53 (2001).

⁶ Robert S. Mueller III, *The FBI's New Mission: Preventing Terrorist Attacks While Protecting Civil Liberties* (Address of the Director of the Federal Bureau of Investigation on the Occasion of the Jackson H. Ralston Prize Ceremony), 39 STAN. J. INT'L L. 117, 120 (2003).

⁷ See OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, THE FEDERAL BUREAU OF INVESTIGATION'S COMPLIANCE WITH ATTORNEY GENERAL'S INVESTIGATIVE GUIDELINES 67 (2005) [hereinafter OIG COMPLIANCE REPORT], <http://www.usdoj.gov/oig/special/0509/final.pdf>; see also Jonathan Finer & Dan Eggen, *Two Leaders of Mosque Arrested in Albany Slings; Pair Is Held in Alleged Plot to Sell Grenade Launcher*, WASH. POST, Aug. 6, 2004, at A3; Caryle Murphy, *Informant's Fire Brings Shadowy Tule; Yemeni Man Helped, Squabbled with FBI*, WASH. POST, Nov. 21, 2004, at A1; Shelley Murphy, *FBI Finds Terror Threat Was Fabricated; Tipster Suspected of Tie to Smuggling*, BOSTON GLOBE, Jan. 26, 2005, at A1 [hereinafter Murphy, *Tipster*]; Jo Napolitano, *Man Arrested in Chicago in Connection with Truck-Bomb Plot*, N.Y. TIMES, Aug. 6, 2004, at A10.

⁸ See *infra* notes 105–212 and accompanying text.

⁹ See *infra* notes 28–56 and accompanying text.

¹⁰ See *infra* notes 50–56 and accompanying text.

¹¹ See *infra* notes 57–72 and accompanying text.

which federal agents should handle confidential informants in criminal investigations.¹²

When conducting national security investigations, however, federal agents have broader discretion regarding the use of informants.¹³ A 1981 Executive Order grants authority to the FBI and other agencies to collect domestic national security intelligence when the target of the investigation is an agent of a foreign power.¹⁴ Furthermore, an act of Congress—the Foreign Intelligence Surveillance Act of 1978 (“FISA”)—sets forth procedures for investigating an agent of a foreign power that depart from the requirements of a criminal search or surveillance warrant.¹⁵ Under these provisions, federal agents may initiate electronic surveillance or even physical searches without following ordinary warrant procedures, and as a result, courts are less involved in supervising the use of informants.¹⁶ Additionally, new guidelines from the Attorney General relating to national security investigations effectively remove the restrictions placed on federal agents when it comes to handling informants.¹⁷

Part I of this Note introduces the body of law governing the use of informants in criminal investigations.¹⁸ Part II discusses the role of informants in the context of national security and examines the differences between the two bodies of law.¹⁹ In national security matters, if the target of an investigation can be classified as an agent of a foreign power, the range of investigative techniques available to the FBI and other agencies is much more extensive than in criminal investigations.²⁰ Furthermore, the legal protections available to criminal defendants become irrelevant if no criminal prosecution results from an intelligence investigation.²¹ Part III considers whether these differences are appropriate, in light of concerns about concentrated execu-

¹² See *infra* notes 73–104 and accompanying text.

¹³ See *infra* notes 105–212 and accompanying text.

¹⁴ Exec. Order No. 12,333, §§ 2–5, 3 C.F.R. 200, 212 (1982), *reprinted in* 50 U.S.C. § 401 note (2000); see *infra* notes 122–135 and accompanying text.

¹⁵ See Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 18 U.S.C. §§ 2511, 2518, 2519, 50 U.S.C. §§ 1801–1811, 1821–1829, 1841–1846, 1861–1862, 1871 (2000 & Supp. III 2003)) [hereinafter FISA], *amended by* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, 118 Stat. 3638; *infra* notes 136–175 and accompanying text.

¹⁶ See *infra* notes 105–175 and accompanying text.

¹⁷ See *infra* notes 176–212 and accompanying text.

¹⁸ See *infra* notes 24–104 and accompanying text.

¹⁹ See *infra* notes 105–212 and accompanying text.

²⁰ See *infra* notes 105–212 and accompanying text.

²¹ See *infra* notes 105–212 and accompanying text.

tive power and infringement upon individual privacy.²² Although these policies reflect a legitimate, elevated fear of the threat from foreign terrorism, they also open the door to increased and largely unsupervised use of confidential informants acting as spies within the United States.²³

I. INFORMANTS IN THE CRIMINAL CONTEXT

The U.S. Constitution provides criminal defendants with certain protections regarding information provided by confidential informants.²⁴ Guidelines issued by the Attorney General also limit the ways in which confidential informants may be utilized in criminal investigations.²⁵ This Part discusses the standard of review for information provided by informants that is used to support a search warrant or an application for electronic surveillance, in addition to other constitutional protections associated with the use of informants in criminal investigations.²⁶ It then introduces the Attorney General's guidelines on the use of confidential informants.²⁷

A. Search Warrants and Applications for Electronic Surveillance

The Fourth Amendment states that search warrants shall issue only upon a showing of "probable cause."²⁸ A judge or other magistrate must review an application for a search warrant and determine that there is probable cause to believe that evidence of a crime exists in a particular place before issuing the warrant.²⁹ Police officers often seek to establish probable cause for a search warrant based on information provided by confidential informants.³⁰ In a pair of cases from the 1960s—*Spinelli v. United States* and *Aguilar v. Texas*—the U.S. Supreme Court developed a two-prong test for determining whether information provided by a confidential informant is sufficient to establish

²² See *infra* notes 213–254 and accompanying text.

²³ See *infra* notes 105–254 and accompanying text.

²⁴ See *infra* notes 28–72 and accompanying text.

²⁵ See *infra* notes 73–104 and accompanying text.

²⁶ See *infra* notes 28–104 and accompanying text.

²⁷ See *infra* notes 28–104 and accompanying text.

²⁸ U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . ."); see *Spinelli v. United States*, 393 U.S. 410, 416–19 (1969); *Aguilar v. Texas*, 378 U.S. 108, 114 (1964).

²⁹ See *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

³⁰ BLOOM, *supra* note 1, at 38–39.

probable cause for a search warrant.³¹ One prong of the *Aguilar-Spinelli* test required that the informant have an actual basis of knowledge of criminal activity, as demonstrated by a showing of specific facts.³² The other prong required a demonstration to a judge that the informant is a credible source.³³ The two-prong *Aguilar-Spinelli* test was used for years, and a deficiency in either prong was enough to undermine a finding of probable cause.³⁴

The Court later modified this rule in the 1983 case of *Illinois v. Gates* by adopting a "totality of the circumstances" approach.³⁵ Under *Gates*, the task of the magistrate issuing the warrant is to make a practical, commonsense decision as to whether probable cause exists for purposes of the Fourth Amendment, taking into account both of the *Aguilar-Spinelli* factors—basis of knowledge of criminal activity and the credibility of the informant—such that a "fair probability [exists] that contraband or evidence of a crime will be found in a particular place."³⁶ By not requiring strict adherence to either of the *Aguilar-Spinelli* prongs, this test makes it easier for the police to obtain search warrants based on information provided by confidential informants.³⁷ Under *Gates*, however, courts still are involved with evaluating the credibility of informants used to establish probable cause in a search warrant affidavit.³⁸

Even with the *Gates* constitutional requirement, it is possible for police officers to fabricate the existence of informants in order to obtain a search warrant, because it is difficult to demonstrate that a police officer is lying in a search warrant application.³⁹ The Supreme Court has generally held that the identity of an informant need not be disclosed in a warrant application, even where the defendant challenges the probable cause determination.⁴⁰ In order to get a hearing to determine the veracity of a sworn statement in a search warrant affidavit, a defendant first must make a substantial preliminary show-

³¹ See *Spinelli*, 393 U.S. at 416–19; *Aguilar*, 378 U.S. at 114.

³² See *Spinelli*, 393 U.S. at 416–19; *Aguilar*, 378 U.S. at 114.

³³ See *Spinelli*, 393 U.S. at 416–19; *Aguilar*, 378 U.S. at 114.

³⁴ See BLOOM, *supra* note 1, at 39.

³⁵ 462 U.S. at 238. The stricter *Aguilar-Spinelli* test is still used in some states, including Massachusetts. See *Commonwealth v. Upton*, 476 N.E.2d 548, 556–58 (Mass. 1985).

³⁶ *Gates*, 462 U.S. at 238.

³⁷ See *id.*; *Spinelli*, 393 U.S. at 416–19; *Aguilar*, 378 U.S. at 114.

³⁸ See *Gates*, 462 U.S. at 239 ("Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others.").

³⁹ See *Franks v. Delaware*, 438 U.S. 154, 155–56 (1978).

⁴⁰ See *McCray v. Illinois*, 386 U.S. 300, 305 (1967).

ing that a false statement was made knowingly and intentionally, or with reckless disregard for the truth.⁴¹ This high standard makes it difficult to convince a judge of the possibility that a police officer might be lying in a warrant affidavit, and serves as an obstacle to getting a hearing to challenge the veracity of the officer's statement.⁴² Although it is impossible to know exactly how often the police invent informants to obtain search warrants, evidence suggests that "testilying" does occur in the world of law enforcement.⁴³ Nevertheless, the fact that a court must at least review a warrant application, which would include information provided by informants, still provides an independent check on law enforcement discretion.⁴⁴

In addition to physical searches of places or people, law enforcement agents also conduct electronic surveillance in criminal investigations, including methods such as wiretapping a phone or bugging a room.⁴⁵ Like physical searches and seizures, electronic surveillance falls within the ambit of the Fourth Amendment protection against unreasonable searches and seizures.⁴⁶ In the 1967 case of *Katz v. United States*, the U.S. Supreme Court held that a warrantless listening device used in a telephone booth violated the Fourth Amendment protection against unreasonable searches.⁴⁷ Famously declaring that "the Fourth Amendment protects people, not places," the Court held that an individual has an expectation of privacy in communications made over the telephone and that therefore government agents may not employ wiretaps without a warrant supported by probable cause.⁴⁸ However, *Katz* explic-

⁴¹ *Franks*, 438 U.S. at 155-56.

⁴² *See id.*

⁴³ BLOOM, *supra* note 1, at 43.

⁴⁴ *See* *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 317 (1972) ("The Fourth Amendment contemplates a prior judicial judgment This judicial role accords with our basic constitutional doctrine that individual freedoms will best be preserved through a separation of powers and division of functions among the different branches and levels of Government.") (footnote and citation omitted).

⁴⁵ *See* 50 U.S.C. § 1801(f) (2000 & Supp. III 2003) (defining electronic surveillance, for the purposes of FISA, as the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication). Electronic surveillance may also include the use of telephonic "pen registers" and "trap and trace devices." *See* 50 U.S.C. § 1841 (2000).

⁴⁶ *See* *Katz v. United States*, 389 U.S. 347, 348 (1967).

⁴⁷ *Id.* at 359.

⁴⁸ *Id.* at 351, 359.

itly left open the question of whether warrantless wiretapping would be permitted in situations involving national security.⁴⁹

After *Katz*, Congress enacted the Omnibus Crime Control and Safe Streets Act in 1968.⁵⁰ Title III of the Act permits electronic surveillance under particular conditions.⁵¹ Judicial authorization must be sought for electronic surveillance intended to prevent certain serious crimes, and the law enforcement officer making the Title III application must explain to the judge why other methods of information collection have been tried and failed, or would be dangerous or likely to fail in the given situation.⁵² Title III applications require a showing of probable cause related to serious crimes specifically delineated in the Act.⁵³ With regard to informant reliability, Title III applications are actually subjected to a higher standard of review than ordinary search-or-seizure warrants.⁵⁴ Internal Department of Justice guidelines state a preference that informants supporting Title III applications be qualified under the *Aguilar-Spinelli* test, rather than the more relaxed *Gates* standard.⁵⁵ Such a preference demonstrates a concern by the Department of Justice that electronic surveillance may be even more invasive of liberty than physical searches, because electronic surveillance can occur entirely in secret without notice to the target and can help law enforcement obtain a vast amount of information about the target.⁵⁶

⁴⁹ *Id.* at 358 n.23 ("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 in this case.").

⁵⁰ Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified as amended in scattered sections of 5 U.S.C., 18 U.S.C., 42 U.S.C.), *amended by* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638, *and* Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, 119 Stat. 2960 (2006).

⁵¹ *Id.* § 802, 82 Stat. at 212-23 (codified as amended at 18 U.S.C. §§ 2510-2520 (2000 & Supp. III 2003)); *see infra* notes 52-53 and accompanying text.

⁵² 18 U.S.C. § 2518(1)(c) (2000).

⁵³ *Id.* § 2518(3)(a). A list of offenses for which electronic surveillance may be conducted with a Title III court order appears at 18 U.S.C. § 2516 (2000 & Supp. III 2003), *amended by* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 6907, 118 Stat. at 3774, *and* Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, § 1171(b), 119 Stat. at 3123.

⁵⁴ *See supra* notes 35-38 and accompanying text.

⁵⁵ *See* U.S. DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL: TITLE 9, CRIMINAL RESOURCE MANUAL § 29(C) (1997), *available at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00029.htm [hereinafter CRIMINAL RESOURCE MANUAL.] (citing *Gates*, 462 U.S. 213; *Spinelli*, 393 U.S. 410; *Aguilar*, 378 U.S. 108).

⁵⁶ *See id.*

B. Other Protections and Defenses

Other constitutional amendments also offer some protection to criminal defendants when the prosecution's case is built on evidence obtained from informants. The Sixth Amendment provides protection to the accused once judicial proceedings have commenced.⁵⁷ In the 1964 case of *Massiah v. United States*, the Supreme Court held that the government may not use an informant as an agent to deliberately elicit statements from a suspect after the initiation of judicial proceedings—the point at which the Sixth Amendment right to counsel attaches.⁵⁸ The Supreme Court affirmed the *Massiah* doctrine in the 1980 case of *United States v. Henry*, holding that the government may not deliberately employ jailhouse informants to initiate conversations with other inmates and thereby encourage incriminating statements.⁵⁹ The Sixth Amendment is not violated, however, if a jailhouse informant is merely a passive listener who reports on the incriminating statements of other inmates, but does nothing to elicit those statements intentionally.⁶⁰

The Due Process Clause of the Fourteenth Amendment also protects defendants from the use of certain statements made to informants.⁶¹ Under the "voluntariness" standard, due process requires that the police not use oppressive or coercive conduct to obtain statements from criminal suspects.⁶² The Court has applied the Fourteenth Amendment voluntariness standard to the context of informants acting as government agents, holding that statements made to an informant may be suppressed if the informant is working as an agent of the government and if the statements are coerced by the informant in the scope of that agency.⁶³

⁵⁷ See U.S. CONST. amend. VI ("In all criminal prosecutions, the accused shall enjoy the right . . . to have the Assistance of Counsel for his defence.").

⁵⁸ 377 U.S. 201, 205–06 (1964).

⁵⁹ 447 U.S. 264, 273–74 (1980).

⁶⁰ See *Kuhlmann v. Wilson*, 477 U.S. 436, 459 (1986).

⁶¹ See U.S. CONST. amend. XIV; *Colorado v. Connelly*, 479 U.S. 157, 164 (1986).

⁶² See *Connelly*, 479 U.S. at 164. Although the Due Process Clause of the Fourteenth Amendment applies only to state action, the voluntariness inquiry is the same under the Due Process Clause of the Fifth Amendment, which applies to the federal government. *E.g.*, *Lam v. Kelchner*, 304 F.3d 256, 264 (3d Cir. 2002).

⁶³ See *Arizona v. Fulminante*, 499 U.S. 279, 287 (1991). The Court has also held, however, that the harmless error standard applies to such statements—a standard that makes it less likely that convictions will be reversed when partially based upon coerced incriminating statements made to informants. *See id.* at 295.

Finally, other defenses may be available to criminal defendants when informants are involved, including the doctrines of entrapment and outrageous government conduct.⁶⁴ While not constitutional in origin, these defenses may be invoked under exceptional circumstances to dispose of an indictment altogether.⁶⁵ In the 1992 case of *Jacobson v. United States*, the Supreme Court held that “[g]overnment agents may not originate a criminal design, implant in an innocent person’s mind the disposition to commit a criminal act, and then induce commission of the crime so that the Government may prosecute.”⁶⁶ Thus, a criminal defendant may raise a defense of entrapment where an informant, working as a government agent, actually induces the defendant to commit a crime and where that defendant otherwise lacked the predisposition to commit that crime.⁶⁷

A related defense is outrageous government conduct, which is similar to the defense of entrapment except that it focuses on the conduct of the government rather than on the predisposition of the defendant.⁶⁸ Presumably, there may be circumstances where an informant, acting as a government agent, engages in conduct that is so outrageous during the course of an investigation that it warrants the dismissal of the indictment.⁶⁹ The Second Circuit has expressed reluctance to dismiss indictments based on this defense, however, concluding that it is the province of the executive branch to determine the appropriate bounds of conduct for its investigative agents, including informants.⁷⁰

Alternatively, an individual who is not accused of a crime, but whose rights have been violated by the use of informants, may also seek civil damages from the government. In the 1971 case of *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics*, the Supreme Court held that individuals may sue federal agents for money damages arising from violations of their constitutional rights that occur during the course of an investigation, even when no criminal prosecution results.⁷¹ The *Bivens* doctrine is the common-law analog to 42

⁶⁴ See Schreiber, *supra* note 5, at 344–49.

⁶⁵ See *id.*

⁶⁶ 503 U.S. 540, 548 (1992).

⁶⁷ See *id.* at 548–51.

⁶⁸ See *United States v. Russell*, 411 U.S. 423, 431 (1973). In *United States v. Russell*, the Court suggested that there may be circumstances where the government’s investigatory conduct is so outrageous that dismissal of an indictment may be warranted on due process grounds. *Id.*

⁶⁹ See *id.*

⁷⁰ See *United States v. DeSapio*, 435 F.2d 272, 281–82 (2d Cir. 1970).

⁷¹ See 403 U.S. 388, 397 (1971).

U.S.C. § 1983, which creates a statutory right for individuals to sue state and local government actors for civil rights violations.⁷²

C. "Top Echelon" and the Attorney General's Informant Guidelines

Although the safeguards discussed above exist to protect the rights of individuals from the unscrupulous use of informants by the government, law enforcement agencies, particularly the FBI, exercise significant discretion regarding the use of informants.⁷³ In order to combat organized crime (once the top priority of the Bureau), the FBI developed a highly secretive, effective, and potentially dangerous system for gathering intelligence through informants—the Top Echelon Informant Program.⁷⁴ In the FBI vernacular, Top Echelon ("TE") informants are those who are directly involved with high levels of organized crime and are therefore serious criminals themselves.⁷⁵

The TE Informant Program has its roots in the 1950s, when the FBI began to shift its focus from investigating communism to fighting the Mafia.⁷⁶ In order to gather quality information on the mob, the FBI needed informants, but informants were rare in the Mafia world because members of the organization took oaths requiring them to kill anyone among them who provided information to law enforcement.⁷⁷ As a result, the FBI launched the ambitious TE Informant Program, which sought to recruit active, ranking members of the Mafia as informants, with the government guaranteeing absolute confidentiality regarding their identities in exchange for information.⁷⁸

The TE program existed almost entirely in secrecy until criminal proceedings in Boston in the late 1990s revealed its sordid details.⁷⁹ The ethical and legal challenges facing the FBI in choosing to associate

⁷² See 42 U.S.C. § 1983 (2000); *Bivens*, 403 U.S. at 397.

⁷³ See *infra* notes 74–104 and accompanying text.

⁷⁴ See RALPH RANALLI, *DEADLY ALLIANCE: THE FBI'S SECRET PARTNERSHIP WITH THE MOB* 56–60 (2001).

⁷⁵ See *id.* at 57.

⁷⁶ *Id.* at 48–49.

⁷⁷ *United States v. Salemme*, 91 F. Supp. 2d 141, 287 (D. Mass. 1999) ("Each took an oath swearing, among other things, that he would abide by 'omerta,' the code of silence. On at least two occasions, the inductee promised to kill without hesitation any police informant posing a threat to the Family, even if the informant were his son or brother."), *rev'd in part sub nom.* *United States v. Flemmi*, 225 F.3d 78 (1st Cir. 2000); RANALLI, *supra* note 74, at 55.

⁷⁸ RANALLI, *supra* note 74, at 57–59.

⁷⁹ See *infra* notes 80–85 and accompanying text.

with criminals came to light at that time when Massachusetts District Court Judge Mark L. Wolf conducted a lengthy set of pretrial hearings in the case of *United States v. Salemme*, thereby uncovering the extensive relationship between the FBI and its informants in the Boston area.⁸⁰ According to the court's findings, two of Boston's most notorious organized crime figures, James "Whitey" Bulger and Stephen "The Rifleman" Flemmi, had been acting as TE informants for the FBI for decades.⁸¹ Bulger and Flemmi provided information on the criminal organization La Cosa Nostra (the "LCN") in exchange for the FBI's sanction of their own loan-sharking and gambling activities.⁸² Thus, while their own criminal enterprise (known as the Winter Hill Organization) flourished, Bulger and Flemmi supplied valuable information to the FBI, effectively wiping out their rivals in the LCN.⁸³ The court's findings uncovered a scandal that resulted in the conviction of FBI agent John Connolly for protecting Bulger and Flemmi, his valued informants, and for tipping off Bulger to his eventual indictment.⁸⁴ Flemmi reached a plea agreement for his cooperation in other cases, and Bulger is still a fugitive, currently on the FBI's Top Ten Most Wanted List.⁸⁵

In response to the Boston scandal, Attorney General Janet Reno issued, in January of 2001, a document titled, "Guidelines Regarding the Use of Confidential Informants."⁸⁶ Older versions of informant guidelines had existed in some form since 1976, when they were implemented in an attempt to reform the FBI's investigative techniques in light of revelations of abuses of power by the Bureau.⁸⁷ The Reno review of the guidelines was spurred in large part by evidence of the FBI's mishandling of Bulger and Flemmi, and the resulting guidelines

⁸⁰ See 91 F. Supp. 2d at 175-316. For further discussion of the legal implications of *Salemme*, see BLOOM, *supra* note 1, at 81-105; Schreiber, *supra* note 5, at 330-41.

⁸¹ *Salemme*, 91 F. Supp. 2d at 148-49. For detailed accounts of the Bulger/Flemmi affair, see generally LEHR & O'NEILL, *supra* note 1, and RANALLI, *supra* note 74.

⁸² *Salemme*, 91 F. Supp. 2d at 151-57.

⁸³ *Id.* at 149-57.

⁸⁴ See *United States v. Connolly*, 341 F.3d 16, 19 (1st Cir. 2003).

⁸⁵ See *Connolly*, 341 F.3d at 19, 21; Shelley Murphy & Stephen Kurkjian, *Flemmi Alleges More FBI Payoffs*, BOSTON GLOBE, May 19, 2005, at A1; FBI's Ten Most Wanted Fugitives, <http://www.fbi.gov/mostwanted/topten/fugitives/fugitives.htm> (last visited Mar. 12, 2006).

⁸⁶ OFFICE OF THE ATTORNEY GEN., U.S. DEPT. OF JUSTICE, DEPARTMENT OF JUSTICE GUIDELINES REGARDING THE USE OF CONFIDENTIAL INFORMANTS (2001), <http://www.usdoj.gov/ag/readingroom/ciguidelines.htm> [hereinafter RENO GUIDELINES]; see OIG COMPLIANCE REPORT, *supra* note 7, at 57-58.

⁸⁷ See OIG COMPLIANCE REPORT, *supra* note 7, at 36-59.

were an attempt to correct those mistakes.⁸⁸ The guidelines were re-issued by former Attorney General John Ashcroft in 2002 in substantially similar form to the Reno version (the "Informant Guidelines"); this newer version remains in effect today.⁸⁹

The current Informant Guidelines are applicable to all domestic investigations conducted by agencies within the Department of Justice, including the FBI.⁹⁰ The Guidelines are designed to control the relationship between informants and their government handlers; they establish standards governing the suitability of informants and require a higher-ranking FBI official than the case agent to review annually each informant's file.⁹¹ Additionally, they establish a Confidential Informant Review Committee within the FBI to assess periodically the ongoing suitability of registered informants.⁹² The Guidelines specifically state that the FBI may not withhold the identity of its informants if the information is requested by any federal prosecutor's office.⁹³ Furthermore, the Guidelines describe in detail the kind of behavior that is prohibited between an informant and a federal agent, including a ban on the exchange of gifts or other monetary payments without specific approval.⁹⁴

Another major restriction imposed by the Informant Guidelines concerns immunity.⁹⁵ The Informant Guidelines state that federal law enforcement agents may not immunize informants from prosecution for specific crimes, nor authorize the commission of certain future crimes, in exchange for information—at least, not without prior approval of an official within the Department of Justice.⁹⁶ Furthermore, the Guidelines prevent agents from making, without prior written approval from a U.S. Attorney's office, "any promise or commitment . . .

⁸⁸ See *id.*

⁸⁹ See generally OFFICE OF THE ATTORNEY GEN., U.S. DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES REGARDING THE USE OF CONFIDENTIAL INFORMANTS (2002), <http://usdoj.gov/olp/dojguidelines.pdf> [hereinafter INFORMANT GUIDELINES]; RENO GUIDELINES, *supra* note 86.

⁹⁰ See *infra* notes 180–197 and accompanying text.

⁹¹ INFORMANT GUIDELINES, *supra* note 89, at 9.

⁹² *Id.* at 5, 10. Once an individual has been deemed suitable to be a confidential informant, that person is "registered" as such, and certain records on that informant must be kept on file. *Id.* at 11.

⁹³ *Id.* at 5.

⁹⁴ *Id.* at 17.

⁹⁵ *Id.* at 5, 19–24.

⁹⁶ INFORMANT GUIDELINES, *supra* note 89, at 5, 19–24.

that would limit the use of any evidence by the government" against the informant.⁹⁷

These prohibitions in the Informant Guidelines reflect a ruling by the First Circuit in *United States v. Flemmi* regarding "use immunity," or immunity with respect to the fruits of electronic surveillance.⁹⁸ The court held that when an informant offers evidence to support a Title III application, an individual FBI agent does not have the authority to immunize that informant as to any incriminating statements that might later be intercepted in the course of the resulting surveillance.⁹⁹ An agent may promise to keep the identity of the informant confidential, but he or she may not grant any form of immunity without seeking further authorization from an official within the Department of Justice.¹⁰⁰ The Informant Guidelines essentially incorporate this holding.¹⁰¹

A recent review of the FBI's compliance with the Guidelines, conducted by the Office of the Inspector General (the "OIG") and detailed in a report issued in September 2005, found that the Bureau has not adequately supported or implemented the Informant Guidelines.¹⁰² The OIG's comprehensive compliance report noted that the FBI is in the process of considering significant changes to its informant program, and it made several specific recommendations for properly implementing the Informant Guidelines.¹⁰³ The report's findings also indicated the ongoing importance of informants to FBI investigations, as well as the necessity of maintaining and improving procedures for proper oversight of criminal informants.¹⁰⁴

II. INFORMANTS IN THE NATIONAL SECURITY CONTEXT

As discussed in Part I, there are limits on how law enforcement agents may use informants in criminal investigations.¹⁰⁵ When the nature of an investigation involves a threat to national security, however, differ-

⁹⁷ *Id.* at 5. The Supreme Court has held that the government must disclose evidence of any understanding or agreement as to protection from a future prosecution of any witness actually testifying for the prosecution in a criminal trial. *Giglio v. United States*, 405 U.S. 150, 154-55 (1972). Of course, this only matters when informants actually testify. *See id.*

⁹⁸ *See* 225 F.3d at 80-81.

⁹⁹ *Id.*

¹⁰⁰ *Id.* at 87-88.

¹⁰¹ *See* INFORMANT GUIDELINES, *supra* note 89, at 19-25.

¹⁰² *See* OIG COMPLIANCE REPORT, *supra* note 7, at 1, 3, 7-9, 57-58, 63-135.

¹⁰³ *Id.* at 133-35.

¹⁰⁴ *Id.*

¹⁰⁵ *See supra* notes 28-104 and accompanying text.

ent rules apply.¹⁰⁶ Courts have granted the executive branch broad discretion over national security matters.¹⁰⁷ The Supreme Court has left open the issue of whether the Fourth Amendment applies in national security investigations,¹⁰⁸ and several circuit courts of appeals have held that it does not.¹⁰⁹ Consequently, in the field of national security, federal investigative agencies are governed by three alternative sources of authority: a 1981 executive order issued by President Reagan,¹¹⁰ a congressional act from 1978,¹¹¹ and guidelines issued by the Attorney General.¹¹² This Part discusses the role of informants in national security investigations, as construed from these sources of authority.¹¹³

A. Executive Order No. 12,333 and Intelligence Investigations

The President has the fundamental duty to "preserve, protect and defend the Constitution of the United States."¹¹⁴ From this executive duty flows the power of executive agencies to investigate and ultimately defend the country from foreign threats.¹¹⁵ When national security is at stake, courts have granted the federal government's executive branch the authority to act outside the scope of the Fourth Amendment.¹¹⁶ The Supreme Court addressed the scope of the executive power to conduct warrantless searches in national security investigations in 1972

¹⁰⁶ See *infra* notes 107–212 and accompanying text.

¹⁰⁷ See *infra* notes 120–121, 152–155, and accompanying text.

¹⁰⁸ *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 310 (1972).

¹⁰⁹ See *infra* note 121 and accompanying text.

¹¹⁰ Exec. Order No. 12,333, 3 C.F.R. 200 (1982), *reprinted in* 50 U.S.C. § 401 note (2000).

¹¹¹ FISA, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 18 U.S.C. §§ 2511, 2518, 2519, 50 U.S.C. §§ 1801–1811, 1821–1829, 1841–1846, 1861–1862, 1871 (2000 & Supp. III 2003)), *amended by* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, 118 Stat. 3638.

¹¹² OFFICE OF THE ATTORNEY GEN., U.S. DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES FOR FBI NATIONAL SECURITY INVESTIGATIONS AND FOREIGN INTELLIGENCE COLLECTION (U) (2003) [hereinafter NSI GUIDELINES], *available at* <http://www.usdoj.gov/olp/nsiguideines.pdf>; OFFICE OF THE ATTORNEY GEN., U.S. DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND TERRORISM ENTERPRISE INVESTIGATIONS (2002) [hereinafter DOMESTIC SECURITY GUIDELINES], *available at* <http://www.usdoj.gov/olp/generalcrimes2.pdf>.

¹¹³ See *infra* notes 114–212 and accompanying text.

¹¹⁴ U.S. CONST. art. II, § 1; see *Keith*, 407 U.S. at 310 ("Implicit in that duty is the power to protect our Government against those who would subvert or overthrow it by unlawful means.").

¹¹⁵ See *Keith*, 407 U.S. at 310. For a complete discussion of the President's power to defend national security, see generally LOUIS FISHER, *PRESIDENTIAL WAR POWER* (2004).

¹¹⁶ See *infra* notes 117–121 and accompanying text.

in *United States v. U.S. District Court (Keith)*.¹¹⁷ In *Keith*, the Court held that federal law enforcement agents must seek warrants for searches when the target of the investigation is purely "domestic," even when the investigation implicates national security concerns.¹¹⁸ The ruling at the time applied to both physical searches and electronic surveillance.¹¹⁹ However, the *Keith* Court specifically left open the issue of the existence of executive power to conduct warrantless searches or surveillance with respect to the activities of "foreign powers or their agents."¹²⁰ Consequently, it has been left to the U.S. circuit courts of appeals to recognize a limited national security exception to the Fourth Amendment warrant requirement; four courts have done so, although the Supreme Court has not explicitly approved this view.¹²¹

In 1981, President Reagan issued Executive Order No. 12,333, thereby claiming for the executive branch the power to conduct warrantless searches and surveillance of agents of a foreign power.¹²² Within the executive branch, the FBI is the entity primarily responsible for gathering domestic national security intelligence.¹²³ The Executive Order places the FBI in charge of gathering intelligence within the United States, leaving the Central Intelligence Agency (the "CIA") responsible for gathering intelligence abroad.¹²⁴ The FBI thus functions not only as a federal police force, but also as a domestic spy agency.¹²⁵ The Bureau maintains an Office of Intelligence that shares information with other intelligence agencies throughout the federal government.¹²⁶ Other entities within the "intelligence community" of

¹¹⁷ See 407 U.S. at 321; David S. Eggert, Note, *Executive Order 12,333: An Assessment of the Validity of Warrantless National Security Searches*, 1983 DUKE L.J. 611, 622.

¹¹⁸ 407 U.S. at 321.

¹¹⁹ See *id.*

¹²⁰ *Id.*

¹²¹ See *United States v. Truong Dinh Hung*, 629 F.2d 908, 914-16 (4th Cir. 1980), *cert. denied*, 454 U.S. 1144 (1982); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir.), *cert. denied*, 434 U.S. 890 (1977); *United States v. Butenko*, 494 F.2d 593, 603-05 (3d Cir.), *cert. denied sub nom. Ivanov v. United States*, 419 U.S. 881 (1974); *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974); see also Eggert, *supra* note 117, at 623-25.

¹²² Exec. Order No. 12,333, § 2.5, 3 C.F.R. 200, 212 (1982), *reprinted in* 50 U.S.C. § 401 note (2000).

¹²³ *Id.* § 1.14(a), 3 C.F.R. at 210, *reprinted in* 50 U.S.C. § 401 note.

¹²⁴ See *id.* § 1.8, 3 C.F.R. at 205, *reprinted in* 50 U.S.C. § 401 note; *id.* § 1.14(a), 3 C.F.R. at 210, *reprinted in* 50 U.S.C. § 401 note.

¹²⁵ See Mueller, *supra* note 6, at 120.

¹²⁶ *Id.*

the executive branch include the Department of State, the Department of Defense, and the National Security Agency.¹²⁷

Executive Order No. 12,333 grants the Attorney General the power to authorize investigative techniques that otherwise would require a warrant if the Attorney General determines in each case that there is probable cause to believe that the "technique" is directed against a foreign power or an agent of a foreign power.¹²⁸ The Order does not define the term "technique," although it states that "[e]lectronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with that Act, as well as this Order."¹²⁹ Because the language only qualifies the term "technique" by stating that electronic surveillance must be conducted in accordance with FISA, an inference may be drawn that the word "technique" includes electronic surveillance as well as other investigative practices, such as traditional physical searches.¹³⁰ "Foreign intelligence" is defined as "information relating to the capabilities, intentions and activities of foreign powers, organizations or persons."¹³¹ These provisions therefore authorize the FBI, at the direction of the Attorney General, to circumvent the warrant requirement when national security is at risk from a foreign threat.¹³² Such searches must be undertaken for intelligence purposes only, not "law enforcement" purposes—meaning that evidence collected without a warrant would still not be admissible in a criminal prosecution.¹³³

The Executive Order makes no explicit reference to the use of confidential informants, but by eliminating the warrant requirement, it authorizes federal agents to conduct searches based on uncorroborated information from informants, without any concern for satisfying the *Illinois v. Gates* standards for informant use in criminal investigations.¹³⁴ Therefore, under the provisions of Executive Order No. 12,333, intelli-

¹²⁷ Exec. Order No. 12,333, §§ 1.4–1.14, 3 C.F.R. at 202–10, *reprinted in* 50 U.S.C. § 401 note.

¹²⁸ *Id.* § 2.5, 3 C.F.R. at 212, *reprinted in* 50 U.S.C. § 401 note (2000). For a discussion of the term "agent of a foreign power" as defined by FISA, see *infra* notes 147–151 and accompanying text.

¹²⁹ Exec. Order No. 12,333, § 2.5, 3 C.F.R. 200, 212 (1982), *reprinted in* 50 U.S.C. § 401 note.

¹³⁰ See *id.*, *reprinted in* 50 U.S.C. § 401 note.

¹³¹ See *id.* § 3.4(d), 3 C.F.R. at 215, *reprinted in* 50 U.S.C. § 401 note.

¹³² See Exec. Order No. 12,333, § 2.5, 3 C.F.R. at 212, *reprinted in* 50 U.S.C. § 401 note.

¹³³ See *Keith*, 407 U.S. at 318–24; Exec. Order No. 12,333, § 2.5, 3 C.F.R. at 212, *reprinted in* 50 U.S.C. § 401 note.

¹³⁴ See 462 U.S. 213, 238 (1983); Exec. Order No. 12,333, 3 C.F.R. 200, *reprinted in* 50 U.S.C. § 401 note (2000); *supra* notes 28–38 and accompanying text.

gence agencies could act on any information received from informants that they deem credible, without having to demonstrate to an independent court that the informant is reliable or has specific knowledge indicating that terrorist actions are afoot.¹³⁵

B. *The Foreign Intelligence Surveillance Act of 1978*

The *Keith* Court held that the Fourth Amendment warrant requirement does apply in domestic national security investigations.¹³⁶ The case left open, however, the constitutionality of warrantless surveillance of foreign organizations or individuals in national security investigations.¹³⁷ Although circuit courts of appeals have subsequently recognized an exception to the Fourth Amendment warrant requirement in national security investigations, the precise scope of executive authority in such cases has not been defined by the Supreme Court or the circuits.¹³⁸ In the 1952 Supreme Court case *Youngstown Sheet & Tube Co. v. Sawyer (Steel Seizure)*, Justice Jackson expressed the classic articulation of the inherent power of the executive and its relationship to congressional authority.¹³⁹ Where the President acts pursuant to an "express or implied authorization of Congress," Jackson wrote, "his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate."¹⁴⁰ Although there may be a "zone of twilight" where Congress and the executive branch have concurrent authority, once Congress expresses its will on a subject, the President is bound by the legislative action.¹⁴¹ As to the executive branch's power to conduct electronic surveillance and other forms of searches in national security investigations—a "zone of twilight" of concurrent presidential and congressional authority—Congress expressed its will in the Foreign Intelligence Surveillance Act of 1978.¹⁴²

Enacted partially as a response to the *Keith* decision, FISA was designed to provide procedures for obtaining prior judicial approval of

¹³⁵ See generally Exec. Order No. 12,333, 3 C.F.R. 200, reprinted in 50 U.S.C. § 401 note.

¹³⁶ 407 U.S. at 320–21.

¹³⁷ See *id.* at 321–22; see also Eggert, *supra* note 117, at 623.

¹³⁸ See *supra* notes 118–121 and accompanying text.

¹³⁹ 343 U.S. 579, 634–55 (1952) (Jackson, J., concurring).

¹⁴⁰ *Id.* at 635.

¹⁴¹ See *id.* at 637.

¹⁴² Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 18 U.S.C. §§ 2511, 2518, 2519, 50 U.S.C. §§ 1801–1811, 1821–1829, 1841–1846, 1861–1862, 1871 (2000 & Supp. III 2003)), amended by Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, 118 Stat. 3638; see also *In re Sealed Case* Nos. 02-001, 02-002, 310 F.3d 717, 719 (FISA Ct. Rev. 2002).

electronic surveillance in national security matters.¹⁴³ In ordinary criminal investigations, Title III court orders must be obtained from a federal district court in order to perform electronic surveillance.¹⁴⁴ But Title III did not address the issue of whether warrants for electronic surveillance are required in national security cases.¹⁴⁵ FISA created the Foreign Intelligence Surveillance Court (the "FISC"), a special court that operates in secret, to issue warrants for electronic surveillance in national security matters.¹⁴⁶ Federal agents may apply directly to the FISC for authorization to conduct electronic surveillance against an "agent of a foreign power" without having to make an application in open federal district court.¹⁴⁷ FISA defines an "[a]gent foreign power" as any person who "engages in clandestine intelligence activities in the United States contrary to the interests of the United States" on behalf of a foreign power.¹⁴⁸ The term "agent of a foreign power" is also used in Executive Order No. 12,333, but it is not defined there; because the terms of the Order itself require adherence with FISA, the Order's definition of this term is evidently the same as that in FISA.¹⁴⁹ An FISC judge may issue an order for electronic surveillance upon finding probable cause that the target is an agent of a foreign power.¹⁵⁰ Because

¹⁴³ See Eggert, *supra* note 117, at 638.

¹⁴⁴ See 18 U.S.C. § 1518 (2000); *supra* notes 50–56 and accompanying text.

¹⁴⁵ See *supra* notes 50–56 and accompanying text.

¹⁴⁶ 50 U.S.C. § 1803(a) (2000 & Supp. III 2003); see *In re Sealed Case*, 310 F.3d at 719.

¹⁴⁷ 50 U.S.C. § 1804(a)(1)(A) (2000); see *id.* § 1801(b) (defining "[a]gent of a foreign power"), amended by Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 6001, 118 Stat. 3638, and USA PATRIOT Authorization and Improvement Act of 2005, Pub. L. No. 109-177, § 103, 120 Stat. 192 (2006). In 2004, Congress inserted subsection (b)(1)(C) in 50 U.S.C. § 1801, adding to the definition of "[a]gent of a foreign power" any person other than a U.S. person who "engages in international terrorism or activities in preparation therefore." Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 6001(a), 118 Stat. 3638, 3742 (to be codified at 50 U.S.C. § 1801(b)(1)(C)), amended by USA PATRIOT Authorization and Improvement Act of 2005, Pub. L. No. 109-177, § 103, 120 Stat. 192 (2006). This subsection is scheduled to expire on December 31, 2009, along with provisions of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act"). See USA PATRIOT Authorization and Improvement Act of 2005, Pub. L. No. 109-177, § 103, 120 Stat. 192 (2006).

¹⁴⁸ 50 U.S.C. § 1801(b); see *supra* note 147 and accompanying text.

¹⁴⁹ Exec. Order No. 12,333, § 2.5, 3 C.F.R. 200, 212 (1982), *reprinted in* 50 U.S.C. § 401 note (2000).

¹⁵⁰ 50 U.S.C. § 1805(a). If the target of the surveillance is a U.S. citizen or otherwise a legal resident of the United States, then there must be probable cause to believe that the target's activities involve espionage or other similar conduct in violation of the criminal statutes of the United States, and the surveillance application must not rely solely upon the basis of speech, association, and other activities protected by the First Amendment. *Id.*

an agent of a foreign power is defined as someone "other than a United States person" operating "in the United States," FISA is not concerned with surveillance conducted against aliens in foreign lands.¹⁵¹

Because Congress has specifically granted the executive limited powers to conduct electronic surveillance and even physical searches without a warrant within the United States in national security investigations through FISA, there is a presumption, under Justice Jackson's formula in *Steel Seizure*, that such conduct is constitutional.¹⁵² Indeed, the electronic surveillance provisions of FISA have been upheld as constitutional by the Second Circuit Court of Appeals.¹⁵³ And although the Supreme Court has never explicitly upheld warrantless physical searches in national security cases, the Fourth Circuit has recognized a general national security exception to the warrant requirement for conducting foreign intelligence surveillance—meaning that such surveillance lies outside the scope of the Fourth Amendment.¹⁵⁴ Therefore, FISA, and not Fourth Amendment caselaw, provides the primary external check on the investigatory methods of the executive branch in national security matters.¹⁵⁵

C. FISA Mechanics and Informants

Although FISA requires prior judicial approval of electronic surveillance in foreign intelligence investigations in most instances, warrantless surveillance may be authorized directly by the Attorney General if certain procedures are followed.¹⁵⁶ Under § 1802(a), the Attorney General may authorize warrantless electronic surveillance for up to one year if it is directed solely against a foreign power and there is

§ 1801(b); 50 U.S.C.A. § 1805(a)(3)(A) (West 2001 & Supp. 2005); see *supra* note 147 and accompanying text.

¹⁵¹ 50 U.S.C. § 1801(b) (emphasis added); see *supra* note 147 and accompanying text; see also *United States v. Verdugo-Urquidez*, 494 U.S. 259, 271–72 (1990) (holding that the protections of the Fourth Amendment do not extend to non-citizens in foreign lands lacking "substantial connection" with the United States). By contrast, the Court held in *United States v. Verdugo-Urquidez* that once an alien lawfully enters and resides in this country, he or she becomes invested with the rights guaranteed by the Constitution, including the full protections of the Fourth Amendment. 494 U.S. at 271–72. What *Verdugo-Urquidez* leaves ambiguous is what constitutes a "substantial connection" for illegal aliens inside or outside the territorial jurisdiction of the United States. See *id.*

¹⁵² See *Steel Seizure*, 343 U.S. at 634–37 (Jackson, J., concurring); *supra* notes 136–151 and accompanying text.

¹⁵³ See *United States v. Duggan*, 743 F.2d 59, 71–76 (2d Cir. 1984).

¹⁵⁴ See *Truong Dinh Hung*, 629 F.2d at 914–16.

¹⁵⁵ See *supra* notes 136–154 and accompanying text.

¹⁵⁶ See 50 U.S.C.A. § 1802(a) (West 2001 & Supp. 2005).

no substantial likelihood that communications of a U.S. person will be intercepted.¹⁵⁷ The Attorney General is required, however, to provide certification of such action to the FISC immediately after ordering the surveillance.¹⁵⁸ FISA also provides the Attorney General with "emergency" power to initiate electronic surveillance without prior judicial approval under § 1805 if an application is made to the FISC within seventy-two hours of the initiation of surveillance.¹⁵⁹ Although these provisions act as a limitation on the kinds of monitoring that federal agents may conduct, they do allow for some degree of warrantless surveillance.¹⁶⁰

Under FISA, law enforcement may also perform physical searches without a warrant under certain circumstances.¹⁶¹ As amended in 1994, FISA grants the Attorney General the power to authorize warrantless physical searches for up to one year to acquire foreign intelligence information, where the search is directed solely at property in the open and exclusive control of a foreign power and there is no substantial likelihood that a U.S. person will be targeted in the search.¹⁶² Just as with electronic surveillance, the Attorney General must submit certification of warrantless physical searches to the FISC immediately after they occur.¹⁶³ Federal agents also may apply for FISA warrants for physical searches, just as they may apply for electronic surveillance warrants.¹⁶⁴

Like Executive Order No. 12,333, FISA does not specifically refer to the use of confidential informants.¹⁶⁵ In ordinary search warrants and Title III applications, informants are frequently cited as sources of information to establish probable cause.¹⁶⁶ Presumably, then, information provided by confidential informants is likewise used to obtain FISA warrants.¹⁶⁷ Unlike in the ordinary warrant and Title III application context, however, the precise standard applied by the FISC to informant qualification is not known because the court operates in

¹⁵⁷ 50 U.S.C. § 1802(a)(1) (2000).

¹⁵⁸ *Id.* § 1802(a)(3).

¹⁵⁹ 50 U.S.C. § 1805(f) (Supp. III 2003).

¹⁶⁰ *See supra* notes 156–159 and accompanying text.

¹⁶¹ 50 U.S.C.A. §§ 1822, 1823(a) (West 2001 & Supp. 2005).

¹⁶² *Id.* §§ 1822, 1823(a).

¹⁶³ *Id.* §§ 1802(a)(3), 1821(4)(D), 1822(a)(1).

¹⁶⁴ *See id.* §§ 1823–1824.

¹⁶⁵ *See id.* §§ 1801–1811, 1821–1829, 1841–1846, 1861–1862, 1871.

¹⁶⁶ *See supra* notes 28–56 and accompanying text.

¹⁶⁷ *See supra* notes 28–56 and accompanying text.

secret.¹⁶⁸ Moreover, since FISA was enacted, only one case has been appealed to the special Foreign Intelligence Surveillance Court of Review, resulting in just one published opinion, and this opinion did not address informants.¹⁶⁹ However, an internal FBI guidance memo shows that the FBI has adopted a “totality-of-the-circumstances” approach as its standard for informant qualification in FISA applications—a standard that comports with the Fourth Amendment requirement established in *Gates*.¹⁷⁰ Although the Justice Department recommends the *Aguilar-Spinelli* standard for Title III applications, the FBI does not suggest this stricter standard in FISA applications.¹⁷¹ Precisely because it operates in secret, one could argue that it would make sense for the FISC to require a *higher* standard for informant qualification than the *Gates* “totality” approach, for there is no need to protect the secret identity of informants in FISA applications.¹⁷² On the other hand, the interest in protecting national security by allowing the surveillance favors a lower quantum of proof for securing the ability to conduct surveillance—an interest perhaps reflected in the fact that in calendar years 2003 and 2004, a combined 3485 FISA warrant applications were made, and only four were denied.¹⁷³ But if and when the Attorney General authorizes warrantless searches or surveillance, there is no prior judicial review of the credibility of the informants providing the basis for investigative activities.¹⁷⁴ In such cases,

¹⁶⁸ See *supra* note 146 and accompanying text.

¹⁶⁹ See *In re Sealed Case*, 310 F.3d at 719.

¹⁷⁰ See FBI Office of Gen. Counsel, What Do I Have to Do to Get a FISA?, at 2–3, <http://www.epic.org/privacy/terrorism/fisa/fisa-recipe.pdf> (last visited Mar. 20, 2006); see also Elec. Privacy Info. Ctr., Foreign Intelligence Surveillance Act Resource Page, <http://www.epic.org/privacy/terrorism/fisa/> (last visited Mar. 20, 2006) (explaining that the Electronic Privacy Information Center obtained the internal FBI guidance memo under a Freedom of Information Act request). According to this document, “in judging the reliability of the information presented by the government, look to the totality of the information and consider its reliability on a case-by-case basis.” See FBI Office of Gen. Counsel, *supra*, at 3. The document specifically refers to *Gates* as “instructive.” *Id.*; see *Gates*, 462 U.S. at 238.

¹⁷¹ See CRIMINAL RESOURCE MANUAL, *supra* note 55, § 29(C); *supra* note 170 and accompanying text.

¹⁷² See *Gates*, 462 U.S. at 238.

¹⁷³ WILLIAM E. MOSCHIELLA, OFFICE OF THE ASSISTANT ATTORNEY GEN., 2004 ANNUAL FOREIGN INTELLIGENCE SURVEILLANCE ACT REPORT TO CONGRESS (2005), available at <http://www.usdoj.gov/oipr/readingroom/2004fisa-ltr.pdf>; WILLIAM E. MOSCHIELLA, OFFICE OF THE ASSISTANT ATTORNEY GEN., 2003 ANNUAL FOREIGN INTELLIGENCE SURVEILLANCE ACT REPORT TO CONGRESS (2004), available at <http://www.usdoj.gov/oipr/readingroom/2003fisa-ltr.pdf>.

¹⁷⁴ See *supra* notes 156–171 and accompanying text.

federal agents are bound only by internal Department of Justice investigative guidelines.¹⁷⁵

D. *The Attorney General's Domestic Security Guidelines*

Former Attorney General John Ashcroft issued several sets of guidelines in 2002 and 2003 governing the investigative practices in both domestic and foreign national security investigations.¹⁷⁶ These guidelines represent the executive branch's internal controls over investigative methods used by the FBI and other agencies, and they are most relevant to an agent's day-to-day investigative authority.¹⁷⁷ Unsurprisingly, the Bureau has a freer hand in national security investigations than in criminal investigations, particularly when the target of the investigation is an agent of a foreign power.¹⁷⁸ These guidelines, while not legally binding, are evidence of the policy choices that the administration of President George W. Bush has made regarding the utilization of confidential informants.¹⁷⁹

The Informant Guidelines are not applicable to investigations of foreign intelligence, since, by their own terms, they apply only to domestic criminal investigations and prosecutions.¹⁸⁰ They do not apply to the use of informants in foreign countries, unless the informant is reasonably likely to be called as a witness in a domestic case.¹⁸¹ Nor do the Informant Guidelines apply to the use of confidential informants in foreign intelligence or foreign counterintelligence investigations.¹⁸²

More recent guidelines address national security investigations specifically.¹⁸³ On May 30, 2002, Ashcroft introduced an updated set of Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (the "Domestic Security Guidelines").¹⁸⁴ The terrorism provisions in the Domestic Security Guidelines are applicable to the FBI's investigations of groups that originate and operate inside the United States.¹⁸⁵ The Domestic Security Guidelines state that they

¹⁷⁵ See *infra* notes 176–197 and accompanying text.

¹⁷⁶ See OIG COMPLIANCE REPORT, *supra* note 7, at 17, 22–23.

¹⁷⁷ See *id.*

¹⁷⁸ See *infra* notes 180–212 and accompanying text.

¹⁷⁹ See *infra* notes 180–212 and accompanying text.

¹⁸⁰ INFORMANT GUIDELINES, *supra* note 89, at 1.

¹⁸¹ *Id.*

¹⁸² *Id.*

¹⁸³ See *infra* notes 184–212 and accompanying text.

¹⁸⁴ See generally DOMESTIC SECURITY GUIDELINES, *supra* note 112.

¹⁸⁵ See *id.* at ii.

are not intended to supersede any applicable provisions of the Informant Guidelines.¹⁸⁶

In criminal investigations, the Domestic Security Guidelines limit the FBI to investigating completed criminal acts or to collecting criminal intelligence information on an ongoing criminal enterprise.¹⁸⁷ However, neither the Informant Guidelines nor the Domestic Security Guidelines are applicable to foreign intelligence or counterintelligence investigations, or to operations in a foreign country.¹⁸⁸ Investigations of terrorist groups originating internationally but operating within the United States are covered by a separate set of guidelines.¹⁸⁹ Therefore, although the Domestic Security Guidelines limit the scope of FBI investigations into criminal matters and, to a lesser extent, domestic terrorist threats, they do not limit investigations involving international terrorists.¹⁹⁰

The Domestic Security Guidelines basically preserve the Informant Guidelines in domestic criminal investigations, although they relax the conditions under which informants may be engaged.¹⁹¹ The Domestic Security Guidelines set forth the investigative procedures that may be used by FBI agents in preliminary inquiries and full investigations.¹⁹² Agents may begin a preliminary inquiry without even a "reasonable indication" of criminal activity when there is information or an allegation not warranting a full investigation, but still requiring further scrutiny beyond the prompt and limited checking of initial leads.¹⁹³ The development of informants is a method available to agents at the preliminary inquiry stage.¹⁹⁴ The Domestic Security Guidelines are ambiguous as to whether agents at the preliminary inquiry stage may develop new informants or only interview previously established informants.¹⁹⁵ The language authorizes agents to interview "previously established informants, and other sources of information," but the introduction to the Domestic Security Guidelines states that "[o]ther methods, including the development of sources and infor-

¹⁸⁶ *Id.* at 23.

¹⁸⁷ *Id.* at 12.

¹⁸⁸ *Id.* at ii; INFORMANT GUIDELINES, *supra* note 89, at 1.

¹⁸⁹ See *infra* notes 198–212 and accompanying text.

¹⁹⁰ See DOMESTIC SECURITY GUIDELINES, *supra* note 112, at 2–3.

¹⁹¹ See *infra* notes 192–197 and accompanying text.

¹⁹² DOMESTIC SECURITY GUIDELINES, *supra* note 112, at 8–12.

¹⁹³ *Id.* at 8.

¹⁹⁴ *Id.* at 1.

¹⁹⁵ See *id.* at 1, 10.

nants" are available at the preliminary inquiry stage.¹⁹⁶ Allowing agents at the preliminary stage not only to use established informants, but also to develop new ones, means that agents are largely unrestricted in terms of when they may seek and develop informants, although they still must act within the boundaries set forth in the Informant Guidelines.¹⁹⁷

E. *The Attorney General's National Security Investigations Guidelines*

When the target of a national security investigation is "an agent of a foreign power," the Informant Guidelines do not apply at all, at least based on a reading of the Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (the "NSI Guidelines"), introduced on October 31, 2003.¹⁹⁸ The NSI Guidelines apply only to the FBI, and they cover investigations of foreign powers and international terrorist organizations, like Al Qaeda, operating within the United States.¹⁹⁹ Portions of these guidelines are classified.²⁰⁰ The NSI Guidelines afford the FBI very broad power to investigate foreign terrorist organizations operating within the United States.²⁰¹

Executive Order No. 12,333 and FISA essentially authorize the FBI to engage in domestic spying, where the targets of investigation are foreign powers or their agents.²⁰² The NSI Guidelines reflect that authority, granting FBI agents broad power to collect foreign national security intelligence beyond what is acceptable in criminal investigations.²⁰³ The unclassified portions of the NSI Guidelines state that the "scope of authorized activities . . . is not limited to 'investigation' in a narrow sense, such as solving particular cases Rather, these activities also provide critical information needed for broader analytic and intelligence purposes authorized by Executive Order 12333" ²⁰⁴ This passage allows FBI agents to undertake broad intelligence inves-

¹⁹⁶ *Id.*

¹⁹⁷ See DOMESTIC SECURITY GUIDELINES, *supra* note 112, at 1, 10, 23.

¹⁹⁸ See generally NSI GUIDELINES, *supra* note 112.

¹⁹⁹ See *id.* at ii, 1-2.

²⁰⁰ *Id.* at 3-38.

²⁰¹ *Id.* at 1-2, 11.

²⁰² See *supra* notes 122-175 and accompanying text.

²⁰³ NSI GUIDELINES, *supra* note 112, at ii; see *supra* notes 122-175 and accompanying text (discussing Executive Order No. 12,333 and FISA). The FBI's authority to collect intelligence in criminal investigations is outlined in the Domestic Security Guidelines. See *supra* notes 187-197 and accompanying text.

²⁰⁴ NSI GUIDELINES, *supra* note 112, at 11.

tigations, outside the bounds defined for criminal or even domestic terrorism investigations.²⁰⁵

The unclassified portions of the NSI Guidelines are interesting for what they do not say: they make no reference to informants at all.²⁰⁶ Furthermore, the Informant Guidelines themselves state that they are not applicable to foreign intelligence or counterintelligence investigations.²⁰⁷ Therefore, when investigating international terrorist organizations existing or operating within the United States, it seems that the FBI is virtually unrestrained in how it may engage the assistance of informants for the purposes of investigation or intelligence-gathering.²⁰⁸

Furthermore, it appears that individual agents must use their own discretion to determine whether the information they receive implicates a foreign national security threat or a domestic security threat, a decision crucial to determining which set of standards applies to the use of informants.²⁰⁹ Such broad discretion for FBI agents to engage informants without formal guidelines from the Department of Justice may be a necessary measure for fighting the war on terror.²¹⁰ Or it may prove to concentrate too much power in the hands of the executive—a power that is subject to greater constitutional and statutory constraint in the criminal context.²¹¹ In either instance the NSI Guidelines reflect a definitive policy choice by the current administration that no rules should apply to the use of informants when foreign potential terrorists are involved.²¹²

²⁰⁵ See DOMESTIC SECURITY GUIDELINES, *supra* note 112, at 12, 15.

²⁰⁶ See generally NSI GUIDELINES, *supra* note 112.

²⁰⁷ INFORMANT GUIDELINES, *supra* note 89, at 1.

²⁰⁸ See *supra* notes 198–205 and accompanying text.

²⁰⁹ See NSI GUIDELINES, *supra* note 112, at 2–3, 9–10; *supra* notes 183–197 and accompanying text.

²¹⁰ See NSI GUIDELINES, *supra* note 112, at 2–3, 9–10.

²¹¹ See *supra* notes 28–104 and accompanying text.

²¹² See *supra* notes 198–211 and accompanying text. By contrast, the Office of the Inspector General has reiterated the importance of implementing and adhering to the Informant Guidelines in criminal and domestic security investigations. See OIG COMPLIANCE REPORT, *supra* note 7, at 133–35.

III. THE TROUBLE WITH UNSUPERVISED USE OF INFORMANTS IN NATIONAL SECURITY INVESTIGATIONS

A. *Effects of Executive Order No. 12,333, FISA, and the Attorney General's Guidelines*

The combined effect of Executive Order No. 12,333, FISA, and the NSI Guidelines is that, in national security investigations under certain circumstances, the FBI and other investigative agencies currently may engage in electronic surveillance or physical searches without prior judicial approval.²¹³ If the government does not need a warrant, it does not need to follow the informant qualification requirements of *Illinois v. Gates*.²¹⁴ Absent the hindrance of *Gates* and prior judicial approval for a warrant, federal agents can act on the basis of any tip from any informant that they choose, without having to demonstrate to a neutral third party that the informant has a shred of credibility.²¹⁵ Furthermore, unless an intelligence investigation results in a prosecution, most of the protections in place in the criminal context will never be implicated.²¹⁶

Such unilateral discretion over the use of informants by the executive branch, and unregulated discretion of individual federal agents to handle informants, raises several concerns.²¹⁷ For one, agents might become too close to their most valuable informants—shielding them from prosecution to ensure their ongoing productivity, or even accepting bribes from informants and participating in their underworld activities.²¹⁸ This kind of behavior was revealed in the Boston FBI scandal, when it was discovered that FBI agents had protected Whitey Bulger and Stephen Flemmi for decades because of their value as informants against the Italian Mafia.²¹⁹ However, in counterterrorism investigations, this concern seems less significant than in the criminal context because it is difficult to imagine a federal agent protecting or participating in conduct that is truly threatening to national security.²²⁰

Two other concerns merit closer consideration, however, in the sections that follow. The first concern is that using informants as a basis

²¹³ See *supra* notes 128–212 and accompanying text.

²¹⁴ See *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

²¹⁵ See *id.*

²¹⁶ See *supra* notes 28–104 and accompanying text.

²¹⁷ See *supra* notes 156–212 and accompanying text.

²¹⁸ See *supra* notes 73–85 and accompanying text.

²¹⁹ See *supra* notes 73–85 and accompanying text.

²²⁰ See *supra* notes 80–85 and accompanying text.

for electronic surveillance without prior judicial review and approval might violate the privacy of U.S. persons.²²¹ The second is that without a judicial check on the use of informants, the concentration of power in the hands of the executive branch might lead investigative agents to overstep proper boundaries.²²² Each will be discussed in turn.²²³

B. NSA Surveillance and Privacy Concerns

When federal agents conduct electronic surveillance or physical searches in compliance with FISA, their conduct is presumptively constitutional, and a FISC judge must at least be informed of their actions.²²⁴ However, reports have recently surfaced indicating that the administration of President George W. Bush has conducted warrantless electronic surveillance for years at the direction of a secret presidential order, without any sort of judicial notification or authorization.²²⁵ According to these reports, the National Security Agency (the "NSA") has monitored telecommunication data regarding phone calls outside the United States that happen to pass through U.S.-based telephonic "switches."²²⁶ Although this kind of surveillance is not directed at U.S. persons, it is entirely possible that the communications of U.S. citizens will be intercepted in the course of such eavesdropping.²²⁷ The NSA has not conducted this surveillance under the terms of FISA because federal agents desire a degree of speed and flexibility to respond to domestic terror threats that they believe FISA does not provide.²²⁸ The NSA surveillance program thus raises serious privacy concerns for any American using a device as technologically simple as a telephone.²²⁹

²²¹ See *infra* notes 224–254 and accompanying text.

²²² See *infra* notes 239–254 and accompanying text.

²²³ See *infra* notes 224–254 and accompanying text.

²²⁴ See *supra* notes 136–175 and accompanying text.

²²⁵ In a series of articles in December, 2005, the *New York Times* reported that the National Security Agency, acting on a secret 2002 order from the Bush Administration, conducted warrantless electronic surveillance on hundreds of occasions. See James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1; Eric Lichtblau & James Risen, *Eavesdropping Effort Began Soon After Sept. 11 Attacks*, N.Y. TIMES, Dec. 18, 2005, at 31; Eric Lichtblau, *F.B.I. Watched Activist Groups, New Files Show*, N.Y. TIMES, Dec. 20, 2005, at A1; Eric Lichtblau & James Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. TIMES, Dec. 24, 2005, at A1.

²²⁶ Lichtblau & Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, *supra* note 225, at A1.

²²⁷ See *id.*

²²⁸ *Id.*

²²⁹ See *id.*

Whether the executive branch has the inherent power to conduct warrantless searches or surveillance in the interest of protecting national security, beyond the scope of FISA, is debatable.²³⁰ Under Justice Jackson's formula in *Youngstown Sheet & Tube Co. v. Sawyer* (*Steel Seizure*), when Congress has expressed its will on a particular matter that otherwise might exist in the "twilight" zone of concurrent executive authority, the President ought to be bound by the language of the legislation.²³¹ Because Congress has specifically laid out procedures for conducting both electronic surveillance and physical searches under FISA, the executive should be bound to follow those rules.²³² By this rationale, warrantless searches or surveillance within the United States or potentially involving U.S. persons should not take place without at least informing an independent court as to what has occurred.²³³

Evidence suggests, however, that the executive branch has not consistently followed FISA, and the danger of such a practice is that it leaves an independent court completely out of the loop.²³⁴ Although the FISC authorizes the vast majority of surveillance applications, and although FISA substitutes prior authorization with subsequent notification in certain circumstances, at least with surveillance conducted pursuant to FISA, the court exercises some degree of supervision over the activity of the executive.²³⁵ This supervision does not allow federal agents to be the "sole judges of when to utilize constitutionally sensitive means in pursuing their tasks."²³⁶ Whenever one branch of government unilaterally makes decisions affecting the privacy of individual Americans, there is the potential for abuse of discretion and misuse of information.²³⁷ To the extent that informants provide federal agents with information that can lead to unsupervised electronic surveillance by the NSA or other intelligence agencies, the executive branch may once again bypass courts and retain broad discretion in its activities, a situation that presents an undeniable threat to individual privacy.²³⁸

²³⁰ See *supra* notes 136-155 and accompanying text.

²³¹ See 343 U.S. 579, 637 (1952) (Jackson, J., concurring).

²³² See *id.*

²³³ See *id.*; *supra* notes 143-175 and accompanying text.

²³⁴ See *supra* notes 224-229 and accompanying text.

²³⁵ See *supra* notes 136-175 and accompanying text.

²³⁶ *United States v. U.S. Dist. Court* (*Keith*), 407 U.S. 297, 317 (1972).

²³⁷ See *id.*

²³⁸ See *id.*

C. The Power of an Informant's Tip

Another concern with a lack of supervision over the use of informants in investigations is that a single piece of information from an informant has the power to set off a wave of action by law enforcement officials, especially when there is a potential national security threat.²³⁹ One such situation began on January 17, 2005, when an anonymous informant called the California Highway Patrol and told police that he had helped smuggle four Chinese nationals into the United States from Mexico.²⁴⁰ According to the informant, this group was planning to launch an attack with nuclear material on the city of Boston.²⁴¹ The informant was soon apprehended, and he confessed that his claim was fictional and that he had been under the influence of drugs and alcohol at the time he made the call.²⁴² Officials speculated that the motivation behind the tip was vengeance; the informant, it turned out, was actually a professional human smuggler, and the four Chinese nationals were customers who failed to pay him for his services.²⁴³ As a result of the informant's false tip, however, law enforcement agents scrambled across the country, and a nationwide manhunt for the potential Chinese terrorists ensued.²⁴⁴

The informant's tip in this instance did not disrupt a terrorist plot, because no such plot existed.²⁴⁵ But a great deal of resources was expended and wasted, and a high degree of anxiety was caused, because of a single phone call from an intoxicated smuggler.²⁴⁶ Because the tip allegedly involved foreign nationals who were supposedly involved in a terrorist threat, and because the authorities were not investigating an actual crime but were seeking intelligence to prevent a future act of terrorism, the ensuing investigation would have been governed by the broad rules set forth in Executive Order No. 12,333, FISA, and the Attorney General's guidelines.²⁴⁷ Consequently, this single tip could have led to warrantless searches across the country, as

²³⁹ See *infra* notes 240–254 and accompanying text.

²⁴⁰ Murphy, *Tipster*, *supra* note 7, at A1.

²⁴¹ *Id.*

²⁴² *Id.*

²⁴³ *Id.*

²⁴⁴ *Id.*

²⁴⁵ Murphy, *Tipster*, *supra* note 7, at A1.

²⁴⁶ *Id.*

²⁴⁷ See *supra* notes 122–135 and accompanying text (discussing Executive Order No. 12,333); *supra* notes 143–175 and accompanying text (discussing FISA); *supra* notes 176–212 and accompanying text (discussing the Attorney General's guidelines).

well as wiretaps and other forms of electronic surveillance, unilaterally approved and performed by the executive branch.²⁴⁸

Because the informant in this case did not seem particularly reliable, a judge or magistrate might not have issued search warrants or authorized electronic surveillance based solely on the information provided in his phone call.²⁴⁹ But because the tip involved an issue of national security, the emergency provisions of FISA meant that a judge was not required to approve any searches law enforcement wanted to conduct.²⁵⁰ Such an example raises the possibility that an individual tipster, or even prankster, could set off a wave of warrantless searches with a single phone call to the local police if that phone call happens to implicate national security concerns.²⁵¹

This incident demonstrates the power that a tip from an informant has to mobilize law enforcement agencies across the country in response to a potential national security threat.²⁵² Otherwise innocent and unsuspecting individuals may have had their homes searched or their phones tapped as a result of one phone call from a drunken smuggler.²⁵³ This incident also demonstrates why the Supreme Court has imposed rules on using informants to obtain search warrants in criminal cases: to prevent law enforcement agents from overstepping their investigatory bounds and intruding on citizens on the basis of uncorroborated or unreliable information from an informant with ulterior motives for dropping a dime.²⁵⁴

CONCLUSION

Law enforcement agents necessarily rely on information provided by unsavory informants in order to solve and prevent crimes. Over time, a set of rules has emerged governing how confidential informants should be used in criminal investigations, in the form of constitutional jurisprudence, congressional legislation, and internal Department of Justice guidelines. In the national security context, however, where the target of the investigation is an agent of a foreign power and the nature

²⁴⁸ See *supra* notes 122–135 and accompanying text (discussing Executive Order No. 12,333); *supra* notes 143–175 and accompanying text (discussing FISA); *supra* notes 176–212 and accompanying text (discussing the Attorney General's guidelines).

²⁴⁹ See *supra* notes 28–56 and accompanying text.

²⁵⁰ See 50 U.S.C. § 1805(f) (Supp. III 2003).

²⁵¹ See *supra* notes 239–250 and accompanying text.

²⁵² See *supra* notes 122–212 and accompanying text.

²⁵³ See *supra* notes 239–244 and accompanying text.

²⁵⁴ See *Gates*, 462 U.S. at 238.

of the investigation is intelligence-gathering rather than law enforcement, the Attorney General may authorize electronic surveillance or physical searches without a warrant. The national security exception to the Fourth Amendment allows for warrantless searches or surveillance on the basis of uncorroborated tips from informants, without any showing to a judge that the information is reliable or that the informant has not provided such information to serve ulterior motives. Furthermore, the President has authorized a program under which the National Security Agency has conducted warrantless electronic surveillance on hundreds of occasions, without following even the minimal requirements of FISA. Such conduct poses a threat to individual privacy of Americans whose communications may be intercepted in the course of such surveillance.

In addition, successive Attorneys General have seen fit to issue guidelines specifically establishing the manner in which federal agents may engage high-level informants. But new guidelines evince a policy decision that federal agents should not be bothered with practical rules for handling confidential informants in national security investigations. The rules established by the Informant Guidelines regarding immunity, payments, bribes, and the nature of relationships between federal agents and their informants do not apply where the target is an international terrorist. For now, this may be a tolerable situation, due to the urgency and difficulty of recruiting informants for counterterrorism investigations. It may well be that the threat posed by foreign terrorists is greater than any threat from homegrown criminals in the past. Yet even if this is true, vigilance is required to ensure that law enforcement agents do not use informants in a way that violates individual privacy or oversteps proper investigative boundaries.

DANIEL V. WARD