INTELLIGENCE AND THE CRIMINAL LAW SYSTEM

Fred F. Manget*

INTRODUCTION

The intersection of intelligence and the criminal law system is like the boundary between tectonic plates. The casual observer does not see much most of the time, but interaction between the two can result in spectacular mountains and valleys. From time to time, there is also the occasional earthquake or volcano. Such upheaval similarly results from two gigantic efforts of the U.S. government that overlap, bang into each other, and sometimes simply grind to a halt in weary attrition.

Those who manage the interaction of the two systems—the U.S. and Assistant U.S. Attorneys, the Criminal Division of the Department of Justice, and the legal counsels to the organizations comprising the intelligence community—have been dealing with fundamental inconsistencies in the two regimes for many years. For example, the end game for the criminal judicial system is to weed out the innocent and subject the guilty to justice. A prosecution looks backward to an event and a trial imposes a judgment on it. The accused are entitled to protections and rules of process based in the Constitution. They are innocent until proven guilty beyond a reasonable doubt. The highest and best use of information for prosecution purposes is evidence supporting the government's case. There is a clear and consistent preference for as much openness and transparency in the criminal process as possible, and all defendants are entitled to discovery of the government's case.

In intelligence, the mere mention of the word, "discovery" sends shivers through intelligence officers. The end game of intelligence is to interpret

* Fred F. Manget is a member of the Senior Intelligence Service and a former Deputy General Counsel of the Central Intelligence Agency. All statements of fact, opinion, or analysis expressed are those of the author and do not reflect the official positions or views of the CIA or any other U.S. Government agency. Nothing in the contents should be construed as asserting or implying U.S. Government authentication of information or Agency endorsement of the author's views. This material has been reviewed by the CIA to prevent the disclosure of classified information.

information objectively and present it to policymakers in a way that assists them in making decisions. The highest and best use of information for intelligence purposes is to get it to national security officials who can use it in a timely way. Intelligence wants to protect the sources or methods that provided the information so new information can be gained, not put them on the witness stand to prove a case in a public proceeding. Intelligence looks forward and provides an estimate of what is happening and will happen. Everyone is guilty until proven innocent, and innocence does not last. Double jeopardy is a fact of life, not a bar to future actions. And plots, betrayal, espionage, hacking, stealing secrets, and deception can be good things.

This article discusses three of the current areas where the interaction of the intelligence and criminal law systems are creating significant issues that will affect policy makers and their decisions on the direction of the two systems.

IN THE BEGINNING THERE WAS THE WALL

When the Central Intelligence Agency (CIA) was created in 1947, the National Security Act of 1947 specifically prohibited it from having law enforcement powers or internal security functions.[1] That formulation remains unchanged in the National Security Act today. It is a manifestation of the deep uneasiness surrounding the creation of the CIA based upon fears that a unified intelligence, security, and police force would tend towards abuses associated with the Gestapo of Nazi Germany and the Soviet Union's KGB. It also reflected the presence of a powerful and long-established federal law enforcement agency, the Federal Bureau of Investigation (FBI), with its own mission, political support, history, and culture.

This policy of separating secret government powers was honored in the past fifty-plus years by the establishment in legal and practical doctrine of a wall of separation between the two worlds. The CIA could not arrest individuals or issue subpoenas. A series of executive orders dating from the mid-1970s prohibited the CIA from conducting electronic surveillance inside the United States.[2] They also prohibited agencies within the intelligence community from collecting foreign intelligence by acquiring information concerning the domestic activities of United States persons.[3] Further, representatives of agencies within the intelligence community could not join or otherwise participate in any organizations within the United States without disclosing their intelligence affiliation, except under procedures approved by the Attorney General.[4]

For its part, the FBI could not conduct espionage overseas. It had to

1. 50 U.S.C. § 403-4a(d)(1) (2005).

2. The prohibition is contained in the current executive order at Exec. Order No. 12,333 § 2.4(a), 46 Fed. Reg. 59,941, 59,950 (Dec. 4, 1981).

3. *Id.* at § 2.3(b), 46 Fed. Reg. at 59,950.

4. *Id.* at § 2.9, 46 Fed. Reg. at 59,952.

coordinate in advance with the CIA its intelligence-related activities and contacts with foreign liaison and security services.[5] The FBI even divided itself between criminal investigative and counterespionage units that operated separately. The Criminal Division of the Department of Justice consistently maintained that it could not share with the intelligence community foreign intelligence information that surfaced in grand jury proceedings because of Federal Rule of Criminal Procedure (FRCrP) 6(e) pertaining to grand jury secrecy. Prosecutors also could not pass to non-law enforcement officials any foreign intelligence information resulting from criminal wiretap surveillance.

In 1980, the Fourth Circuit was asked to draw the line between intelligence and the criminal law in a seminal espionage case.[6] In the 1970s, U.S. government counterintelligence efforts uncovered a U.S. Information Agency employee (Humphrey) who was passing classified diplomatic information to a Vietnamese citizen (Truong) who then passed it to North Vietnamese officials who were negotiating with United States representatives in Paris. The FBI, using a national security rationale rather than a criminal standard under Title III,[7] bugged Truong's apartment and tapped his phone over the course of a number of months. At some point in the surveillance, prosecutors from the Department of Justice began to take an active part in directing the surveillance.

When the issue arose of whether the incriminating evidence surfaced by the surveillance could be admitted in evidence in the government's criminal case against Humphrey and Truong, the trial court in the Eastern District of Virginia crafted a test that came to be a benchmark in legal analysis for over twenty years. The court opined that so long as the primary purpose of the surveillance was collection of national security information relating to activities of a foreign power, the resulting information could be used in the criminal case. But at some point during the surveillance, the primary purpose changed and became collection of information to support a criminal prosecution. The court noted that the involvement of those on the criminal side of the wall (prosecutors) determined the shift in primary purpose. The primary purpose test was born, and several circuits followed *Truong* in applying it in cases where issues of surveillance arose.[8] The U.S. government subsequently used the primary purpose test for many years when trying to determine which set of rules to apply to other activities that involved both law enforcement and

5. NATIONAL SECURITY COUNCIL INTELLIGENCE DIRECTIVE (NSCID) NO. 5, U.S. ESPIONAGE AND COUNTERINTELLIGENCE ACTIVITIES ABROAD (1972). Director of Central Intelligence Directive (DCID) 5/1 (1984) implemented NSCID NO. 5, but it remains classified and unreleased, according to the latest information available to the author.

6. United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980).

7. 18 U.S.C. § 2518 (2005).

8. *E.g.*, United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991). ("Although evidence obtained under FISA subsequently may be used in criminal prosecutions, . . . the investigation of criminal activity cannot be the primary purpose of the surveillance."); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987); United States v. Pelton, 835 F.2d 1067, 1075-76 (4th Cir. 1987).

intelligence interests.[9]

But a number of factors over time caused the wall to develop breaches and translucency, if not transparency. It was apparent from the beginning that although the CIA had no law enforcement powers, it could support law enforcement activities. This became firmly embedded in intelligence law, both in executive order[10] and statute.[11] In the Intelligence Authorization Act for Fiscal Year 1997, a specific and explicit law enforcement authority for the intelligence community was added to the National Security Act. It states that upon the request of a law enforcement agency, elements of the intelligence community may collect information outside the United States about individuals who are not United States persons, notwithstanding the fact that the law enforcement agency intends to use the information collected for purposes of a law enforcement investigation.

It was a two-way street. Other parts of the National Security Act were added that require that other federal agencies "shall expeditiously disclose to the Director of Central Intelligence . . . foreign intelligence acquired . . . in the course of a criminal investigation."[12]

The increasing overlap of targets drove much of this convergence.[13] The crime of espionage has always had an international component,[14] and overlapping CIA and FBI counterintelligence activities are the stuff of legend.[15] Starting in the 1970s, the United States significantly created or expanded other extraterritorial crimes. Crimes under domestic U.S. law could now be committed outside the territory of the United States by foreign nationals. These included aircraft hijacking and piracy,[16] which were tactics of international terrorist groups of intense interest to the intelligence community. Weapons proliferation (especially chemical and biological weapons),[17] international narcotics trafficking,[18] and organized crime[19] also joined the list

9. *See In re* Sealed Case No. 02-001, 310 F.3d 717, 725-27, 743 (FISA Ct. Rev. 2002).

10. Exec. Order No. 12,333 § 2.6, 46 Fed. Reg. 59,941, 59,951 (Dec. 4, 1981).

11. 50 U.S.C. § 403-5a (2005).

12. 50 U.S.C. § 403-5b(a)(1) (2005).

13. "U.S. persons may be authorized targets, and the surveillance is part of an investigative process often designed to protect against the commission of serious crimes such as espionage, sabotage, assassination, kidnapping, and terrorist acts committed by or on behalf of foreign powers. Intelligence and criminal law enforcement tend to merge in this area." S. REP. NO. 95-701 at 10-11 (1978) (relating to the Foreign Intelligence Surveillance Act of 1978).

14. *E.g.*, 18 U.S.C. § 793 (2005). Espionage requires, as an element of the offense, intent or reason to believe that the national defense information acquired is to be used to the injury of the United States or to the advantage of a foreign nation.

15. *See generally* MARK RIEBLING, WEDGE: THE SECRET WAR BETWEEN THE FBI AND THE CIA (1994).

16. 18 U.S.C. § 32 (2005).

17. 18 U.S.C. §§ 175, 229 (2005).

18. 21 U.S.C. § 959 (2005).

19. 18 U.S.C. §§ 1961-1968 (2005).

of illegal activities subject to prosecution in U.S. courts. New crimes without borders, such as cybercrime,[20] developed in tandem with technological innovations. Terrorism crimes also expanded the reach of U.S. criminal law.[21]

The authority of the FBI to operate outside the United States also grew. The Office of Legal Counsel at the Department of Justice issued an opinion in 1989 concluding that the FBI had the authority to override customary or other international law in its extraterritorial law enforcement activities. The FBI could investigate and arrest fugitives in another state without the consent of the host government.[22] Supreme Court cases also expanded the FBI's reach. One held that an extradition treaty was not the exclusive means by which the United States could take custody of a suspect in a foreign country in which he had been apprehended by persons acting on behalf of the United States without regard to the treaty's provisions.[23] Another held that the Fourth Amendment does not apply to the search and seizure of property in a foreign country owned by a nonresident alien who has no "significant voluntary connection" with the United States.[24]

When the Foreign Intelligence Surveillance Act[25] was passed in 1978, the issue of whether information resulting from a foreign intelligence search under its auspices could be used in a criminal case was swiftly litigated and accepted as constitutional.[26]

Other forms of convergence happened, grew, or were mandated. As a result of the reorganization of U.S. counterintelligence that occurred after the Ames espionage affair, a statute was enacted in 1995 that pushed—some say crammed—intelligence community and law enforcement counterintelligence efforts together.[27] That law, among its other provisions, requires intelligence agencies to immediately advise the FBI of any information indicating that classified information may have been disclosed in an unauthorized manner to a foreign power or agent of a foreign power. It also requires prior coordination and consultation between the agencies for any further actions they may take.

In 2001, the USA PATRIOT Act (the Patriot Act) explicitly authorized law enforcement agencies to share with the intelligence community any foreign intelligence information that was Rule 6(e) grand jury information or Title III electronic, wire, and oral interception information which had been generated by

20. 18 U.S.C. § 1030 (2005).

21. 18 U.S.C. §§ 2331-2339D (2005).

22. Authority of the Federal Bureau of Investigation to Override Customary or Other International Law in the Course of Extraterritorial Law Enforcement Activities, 13 Op. Off. Legal Counsel 195 (1989).

23. United States v. Alvarez-Machain, 504 U.S. 655 (1992).

24. United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

25. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-1811 (2005).

26. *E.g.*, United States v. Megahey, 553 F. Supp. 1180 (E.D.N.Y. 1982), *aff'd sub nom.* United States v. Duggan, 743 F.2d 59 (2d Cir. 1984).

27. Intelligence Authorization Act for Fiscal Year 1995, 50 U.S.C. § 402a (2005).

a criminal investigation.[28]

The final blow to the wall was the 2002 opinion of the Foreign Intelligence Surveillance Court of Review, sitting for the first time in history.[29] It was an appeal brought by the U.S. government from a Foreign Intelligence Surveillance Court (FISC) surveillance order imposing a number of restrictions on the government based upon the wall and primary purpose tests. The FISC court opined that it could approve Foreign Intelligence Surveillance Act (FISA) surveillance applications only if the government's objective is not primarily directed toward criminal prosecution of the foreign agents for their foreign intelligence activity. The Court of Review, however, did not agree. It said that at some point in the 1980s ("the exact moment is shrouded in historical mist")[30] the Department of Justice applied the pre-FISA *Truong* analysis to FISA without justification. The court went on to demolish the past practice of finding a primary purpose in order to surmount a wall established by FISA.

Each one of these developments reflects the U.S. government's multi-front attack on particular problems. A current example, terrorism, is a threat being addressed by every significant method of American power: intelligence, law enforcement, diplomatic efforts, and military action. Fusion centers such as the National Counterterrorism Center have been established combining elements of all the above. The intelligence community provides important participation in all Joint Terrorism Task Forces in FBI field offices. Senior FBI agents help manage the CIA's Counterterrorist Center. There is very little call (if any) that a wall should be maintained or resurrected between law enforcement and intelligence activities. In fact, just the opposite is the case. Every major recent review of U.S. intelligence policy and organization has called for increased information sharing, unity of command and control, and removal of barriers to joint and complementary action among U.S. government departments and agencies.[31] The wall is gone.

The question for policy makers and implementers is whether the United States wants to go that far. Do we wish to combine foreign intelligence and criminal law authorities so completely that only the most pure of purposes are separated? On the one hand, efficiency is sacrificed if walls are erected. On the

28. United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered sections of the U.S.C.).

29. *In re* Sealed Case No. 02-001, 310 F.3d 717, 719 (FISA. Ct. Rev. 2002).

30. *Id.* at 727.

31. *See, e.g.*, COMM'N ON INTELLIGENCE CAPABILITIES OF THE U.S. REGARDING WEAPONS OF MASS DESTRUCTION (THE WMD COMMISSION), REPORT TO THE PRESIDENT (2005); NATIONAL COMM'N ON TERRORIST ATTACKS UPON THE U.S., 9/11 COMMISSION REPORT (2004); S. SELECT COMM. ON INTELLIGENCE & H. PERMANENT SELECT COMM. ON INTELLIGENCE, JOINT INQUIRY INTO INTELLIGENCE COMMUNITY ACTIVITIES BEFORE AND AFTER THE TERRORIST ATTACKS OF SEPTEMBER 11, 2001, S. REP. NO. 107-351, H. REP. NO. 107-792 (2d Sess. 2002); COMM'N ON ROLES AND CAPABILITIES OF THE U.S. INTELLIGENCE CMTY. (THE ASPIN-BROWN COMMISSION), PREPARING FOR THE 21ST CENTURY: AN APPRAISAL OF U.S. INTELLIGENCE (1996).

other hand, the national security establishment in the United States is becoming interpenetrated, interconnected, mutually colonized, and jointly co-opted to an extent never seen since the independent civilian intelligence mission was established. Perhaps in threat related areas (such as counterterrorism) the problems of advance warning greatly outweigh the dangers of loss of checks and balances of separate agencies, missions, and authorities. In other areas of convergence (such as narcotics or international organized crime) perhaps the combination is not so critical.

Creation of an agency whose operations would overlap in the middle (where the wall used to be) is another option that could address both policy goals. Commentators have raised the British domestic security service MI-5 as a possible example. It would carry out an intelligence function separate from the law enforcement mission now owned by the FBI and to a lesser extent, the Department of Homeland Security. The United States could locate such a service in either of those two parent organizations, but it would be difficult to maintain the right balance between intelligence and criminal law interests.[32] Nevertheless, the creation of the Director of National Intelligence and the increasing use of perpetual, joint task force centers such as the National Counterterrorism Center (and a nascent counterproliferation center) have made the current re-engineering of the intelligence community an opportunity for rational readjustments.

The United States faces enormous difficulties in creating a comprehensive solution to reconcile division of authority and power for the purpose of checks and balances while simultaneously pushing the divided agencies to cooperate more and more for efficiency and effectiveness.

In the 1990s, a group of FBI legal attaches (Legatts) and CIA station chiefs (COSs) convened at a neutral location overseas to discuss their increasingly converging missions. In one of the sessions, the panel moderator described a scenario in which the Legatt and COS in a fictional country are called by the local internal security service and invited to visit an apartment in which the local police had just arrested a known and wanted terrorist. The apartment contained a lot of computers, files, photographs, and other materials. The discussion diverged into a theological disputation of what was in the apartment, and by implication, who got to do what with it. Was it evidence? Was it intelligence?

The then-general counsel of the FBI, who was observing the meeting, famously ended the disagreement by saying, "It isn't evidence or intelligence,

32. "Appearing [at a panel discussion before the American Enterprise Institute] alongside [U.S. Court of Appeals for the District of Columbia Judge] Silberman, Judge Richard A. Posner of the U.S. Court of Appeals for the 7th Circuit said he believed that crime fighting, rather than intelligence work, 'will always be dominant' in the [FBI] . . . . As a result, Posner said, there is 'really a deep dog and cat incompatibility between criminal and intelligence activities.'" Dan Eggen & Walter Pincus, *Report: FBI Analyst Jobs Remain Vacant*, WASH. POST, May 5, 2005, at A23.

yet. At this point it's just a room full of stuff." But sometimes the "stuff" is both evidence and intelligence, and sometimes it is neither, and sometimes it changes over time.

It is unlikely that the United States will ever again treat the significant problems confronting it with actions that are exclusively oriented toward either intelligence collection or law enforcement (not to mention the possibility of diplomatic or military action). It is therefore not particularly useful to come up with conclusions that argue for awarding sole or even primary jurisdiction to one or the other. There are intelligence aspects of counterterrorism, nuclear proliferation, and narcotics trafficking, as well as law enforcement aspects. There always will be. The challenge for policymakers in these areas is to continually adjust the boundaries to achieve the maximum beneficial effect on reaching the goals of the United States.

Although frustrating to those implementing policy, extensive interaction between the two worlds will continue. The demise of the wall and the now mandatory mutual support between the criminal law system and the intelligence community means that the most important policy decision is whether to create a new institution to bridge the gap. The FBI has announced that it has reoriented itself from crime fighting to terrorism prevention, but it remains at base a law enforcement agency. Grey areas will exist that make the answers to particular situations unclear and conflicting.

In designing the law enforcement and intelligence agencies of the future, architects should consider the historical lessons. The division of authority and power has worked fairly well most of the time to prevent abuses, but not perfectly and not all the time. Fundamental differences between intelligence and the criminal law systems are inherent in their nature and will remain. Policy makers may get the best overall results from boundary adjustments rather than radical surgery. The United States already has an "MI-5" with the needed authorities, personnel, resources, and capabilities: the FBI. The key is for an appropriate part of that organization to have a mission aside from supporting prosecutions.

YOU HAVE THE RIGHT TO REMAIN SILENT

Criminal procedure has created perhaps the most extensive area of interaction between intelligence and the criminal law system. Other commentators have covered this ground with great thoroughness,[33] and the following is only a summary of the many issues that arise.

Intelligence information generally comes into the criminal process in one of two major ways. One is when intelligence collection results in information

33. The best and most comprehensive article is Jonathan Fredman, *Intelligence Agencies, Law Enforcement, and the Prosecution Team*, 16 YALE L. & POL'Y REV. 331 (1998). Fredman is a colleague of the author.

that the law enforcement agency or prosecution believes may be useful in developing the case in chief. Law enforcement agencies routinely receive a significant amount of information in intelligence reports that is for lead purposes only and remains classified. Law enforcement agencies may use it to develop their own independent cases, but not as evidence to be introduced in a public court proceeding. In some cases though, the lead purpose information is significant enough for the prosecutors to want to use it as evidence. In that circumstance, the information is subject to the evidentiary rules governing admission of information in the case in chief.

The second way that intelligence data enters the criminal justice system results from the prosecution's efforts to comply with discovery rules requiring the disclosure to the defense of certain types of information. Federal discovery obligations apply not only to law enforcement agencies but also to other government agencies that are aligned with the prosecution.[34] Alignment occurs when another agency becomes an active participant in the investigation or prosecution of a particular case.[35] The significance of alignment is that in certain areas such as counterterrorism and weapons proliferation, the extensive cooperation between intelligence and law enforcement agencies may put intelligence information squarely in the criminal process.

The discovery rules most significant to intelligence equities are the constitutional requirements of *Brady* and *Giglio*, Federal Rule of Criminal Procedure (FRCrP) 16, and the Jencks Act. *Brady* requires the government to disclose to the defendant any evidence that is material to the guilt or punishment of the accused.[36] *Giglio* requires the same for evidence material to the impeachment of a government witness.[37] Rule 16 requires the government to disclose any relevant written or recorded statement of the defendant within the custody or control of the government, and any documents or tangible objects that are material to the defense, belong to the defendant, or are intended for use in the government's case in chief. The Jencks Act requires the government to disclose any statements of government witnesses within its possession that relate to the witnesses' testimony.[38]

Intelligence information that has a value independent of that connected to prosecution or defense interests is thus immediately at risk when treated under criminal discovery and evidentiary rules. Because of that risk, in the past the U.S. government was faced with what was dubbed "greymail." Greymail is the threat that the defendant will publicly disclose classified information that could damage national security interests of the United States. Where the criminal procedure rules require that the defendant have access to classified materials (a very fact-specific determination), then the government must guess what will be

34. *See, e.g.*, United States v. Brooks, 966 F.2d 1500 (D.C. Cir. 1992).
35. Fredman, *supra* note 33, at 347-48.
36. Brady v. Maryland, 373 U.S. 83 (1963).
37. Giglio v. United States, 405 U.S. 150 (1972).
38. 18 U.S.C. § 3500 (2005).

disclosed and how much damage will occur.

In order to provide a process by which risk of exposure of classified information could be assessed, Congress enacted the Classified Information Procedures Act (CIPA) in 1980.[39] It is procedural rather than substantive, and so does not affect the outcome of whether classified information must be disclosed to the defendant or used in a public proceeding. It does, however, remove the aspects of ambush that dogged prosecutors in previous cases. CIPA requires notice of what classified information the defense intends to use. It allows for the court to hear *in camera* and *ex parte* presentations in order to review classified information and determine if it must be disclosed in order to ensure a fair trial or otherwise meet criminal due process discovery and evidentiary requirements. It also allows the government to propose unclassified substitutions for classified information that would give the defendant the same ability to put on a defense as would the use of the original classified information. Finally, it allows the court to fashion sanctions, including dismissal, in cases where the government refuses to disclose the classified information at issue.

By using the CIPA procedures, the government can get evidentiary rulings from the court on the classified information in advance of public hearings or trials. Once those evidentiary rulings are made, the government then can understand the risk of proceeding with the prosecution and determine what national security damage might occur. CIPA allows a much more rational and informed decision to be made by the government. But it is still not easy.

In 1985, a Lebanese citizen named Fawaz Yunis and several others hijacked Royal Jordanian Airlines flight number 402. Three Americans were on board. In Beirut, the hijackers held a press conference, evacuated the crew and passengers, and blew up the aircraft. They then disappeared into Lebanon. A massive United States effort involving the CIA, the FBI, and the Department of Defense resulted in luring Yunis into international waters in 1987. There, he was arrested by FBI agents, placed upon a series of military aircraft and Navy ships, and transported to Andrews Air Force Base.[40] He subsequently was arraigned in the District of Columbia and charged with air piracy and hostage taking, among other offenses.

Defense counsel and the Department of Justice then conducted an epic discovery battle that was grounded in the CIA's need to protect classified information related to the operation that resulted in Yunis's arrest.[41] Under FRCrP 16(a)(1)(A), defense counsel pressed for copies of all materials related to electronic surveillance of the defendant and a government informant. The

39. 18 U.S.C. app. §§ 1-16 (2005).

40. A fascinating and authoritative account of the operation is contained in the autobiography of the legendary CIA operations officer who was Chief of the DCI (Director of Central Intelligence) Counterterrorist Center at the time. DUANE R. CLARRIDGE, A SPY FOR ALL SEASONS (1997).

41. *See* United States v. Yunis, 867 F.2d 617 (D.C. Cir. 1989).

trial court took the position that the government should be bound by normal rules of discovery that were well known and used in criminal practice. In such cases, it is routine to turn over all such materials related to the government's wiretap or other similar surveillance of a defendant. Yet the threat to classified information was so great that, on the government's interlocutory appeal, the D.C. Circuit held that classified information is not discoverable on a mere showing of theoretical relevance in the face of the government's classified information privilege. The threshold for discovery in that context further requires that defendants seeking classified information may only get information that is at least helpful to their defense or essential to the fair resolution of their cases.[42]

This adjustment of a boundary was helpful to the United States. It still requires a case-by-case consideration of unique facts, however, and does not provide predictability for field operations. Intelligence collectors cannot conduct their activities with one eye looking over their shoulder at a theoretical future prosecution of some individual for some crime that might implicate some intelligence source or method, all to be determined.[43] All of those criminal procedure practices that are second nature to law enforcement agents—chain of custody, Miranda warnings, search warrants—are burdens that can seriously hobble intelligence collection.

Although not as significant, other issues can arise in addition to those involving pre-trial discovery and evidentiary rulings. The circumstances under which a defendant is rendered to a court of competent jurisdiction may become litigated if the defense raises the *Toscanino* exception to the *Ker-Frisbie* doctrine. The *Ker-Frisbie* doctrine (based on two seminal cases)[44] holds that a trial court will not bar a trial based upon the conditions under which the defendant is brought before the court. Even if the defendant is taken into custody and transported before the court in some manner that is arguably unlawful, the court will not dismiss the case so long as the defendant can expect a fair trial before that particular court. *Toscanino*[45] was a Second Circuit decision that created an exception to the *Ker-Frisbie* doctrine. The court in *Toscanino* said that if the conduct of government agents who rendered the defendant to the court's jurisdiction was so outrageous as to shock the conscience of the court, then the court would at least hear defense motions to dismiss based on those conditions.

Should the CIA provide authorized support to a law enforcement agency

42. *See id.* at 623, 625.

43. Stewart Baker, former General Counsel of the National Security Agency (NSA), has commented for a number of years about the inherent and intractable problems of mixing intelligence and law enforcement operations. *See* Stewart A. Baker, *Should Spies Be Cops?*, 97 FOREIGN POL'Y 36, 49 (Winter 1994-1995).

44. Frisbie v. Collins, 342 U.S. 519 (1952); Ker v. Illinois, 119 U.S. 436 (1886).

45. United States v. Toscanino, 500 F.2d 267 (2d Cir. 1974), *reh'g denied*, 504 F.2d 1380 (2d Cir. 1974).

by supplying CIA resources of equipment, personnel, or technical assistance for a clandestine exfiltration or delivery of a prisoner, then it is possible that the conditions of the operation could be litigated. Disclosure of intelligence sources, methods, and sensitive operational activities would inevitably become an issue in such litigation. There has not been much historical success in raising the *Toscanino* defense.[46] But it has been raised.

At a more fundamental level, applying long-established and iron laws of criminal due process to individuals in custody can effectively destroy any value they have as intelligence sources. Rules of discovery and evidence have the most immediate impact on intelligence equities, but criminal due process extends beyond that. For example, the criminal law system wants those in jeopardy of criminal sanctions to have a level playing field. Fundamental notions of what is fair include those enshrined in the U.S. Constitution: the Fifth Amendment right against self-incrimination, and the Sixth Amendment right to legal counsel. Assuming the U.S. government has lawful grounds for incarcerating individuals other than to subject them to criminal trials (such as holding enemy prisoners of war), then such basic elements of criminal law could interpose near-insurmountable barriers to acquiring information about future threats. The last thing an intelligence interrogator wants someone in custody (whether military, foreign police, or FBI) to hear is, "You have the right to remain silent. You have the right to an attorney. If you cannot afford one, one will be appointed for you. . . ." And the last thing a prosecutor wants to read over morning coffee is a headline that says, "U.S. Intelligence May Aid Terrorist Suspect."[47]

Use of the military criminal law system under either the Uniform Code of Military Justice (UCMJ) or the laws of war does not solve the problem of fundamentally different ends. The UCMJ largely mirrors civilian Federal Rules of Criminal Procedure, including a version of CIPA.[48] The Geneva Conventions applicable to those held as prisoners of war (POWs) require name, rank, and serial number only, and POWs may not be forced to provide any further information. They may be asked for and even volunteer further information, but "[n]o physical or mental torture, *nor any other form of coercion*, may be inflicted on prisoners of war to secure from them information of any kind whatever. Prisoners of war who refuse to answer may not be threatened, insulted, or exposed to unpleasant or disadvantageous treatment of any kind."[49] They also must receive regular visits from the Red Cross and

46. *See* 2 JOHN WESLEY HALL, SEARCH AND SEIZURE § 36.7 n.38 (3d ed. 2000).

47. Craig Whitlock, *U.S. Intelligence May Aid Terrorism Suspect*, WASH. POST, May 25, 2005, at A22 (discussing the trial in Germany of accused September 11, 2001, al Qaeda plotter Mounir Motassadeq).

48. MIL. R. EVID. 505.

49. U.S. DEP'T OF ARMY, FIELD MANUAL 27-10, THE LAW OF LAND WARFARE, ¶ 93 (1956) (emphasis added).

packages mailed from home.[50] Stateless individuals presenting a clear and present danger, such as terrorists, and in the past pirates and slave traders, do not fit that system.

The dilemma of terrorist detainees has also become critical. Is a detainee to be treated under rules applicable to defendants in the U.S. civilian criminal law system? Or the military criminal law system? Or those rules established in a *sui generis* tribunal, under principles of the international law of war? Or, is the detainee to be treated as a source of intelligence that could be critical to early warning of attack? Alternatively, is a detainee first an intelligence source, and then later a criminal defendant? Or both, simultaneously? Where does the right to remain silent begin and end?

The scenario that produces the most conflict is the fatal tainting of information necessary for a conviction. The government wants to avoid a trial where evidence is excluded because it was obtained by interrogation that is lawful for national security and intelligence purposes but not for the purpose of developing evidence for a criminal trial.[51]

For policy makers, the issue is how to reconcile application of the criminal law procedural rules and requirements for protection of defendants with intelligence information and activities. Recent decisions of the Supreme Court and lower federal courts have attempted to do so.[52] The results hardly signify a national consensus.[53] Courts are limited in many ways that legislatures are not. The United States should not ask the courts to craft a publicly acceptable and smooth interface between criminal procedural rules and the imperatives of intelligence and national security, in the middle of a shooting war, based only on the facts of a particular case before them, while limited in jurisdiction. That is the work of Congress.

As this article was being written, the Chairman of the Senate Judiciary Committee, Senator Arlen Specter (R-Pennsylvania) issued a public statement announcing hearings to discuss creating clear due process rules for suspected terrorists. One suggestion is to expand the jurisdiction of the Foreign

---

50. *Id.* ¶¶ 147, 148, 206.

51. "'Why don't they just deliver all these people to the immediate custody of the Supreme Court and let them decide what to do with them?' grouses Theodore Olson, the former solicitor general. 'It's a hell of a mess.'" *quoted in* Michael Isikoff & Mark Hosenball, *Got Him, Now What?*, NEWSWEEK, May 16, 2005, at 24, 27.

52. *E.g.*, Hamdi v. Rumsfeld, 542 U.S. 507 (2004). In his dissenting opinion, Justice Scalia makes this point: "The allegations here, of course, are no ordinary accusations of criminal activity. . . . The relevant question, then, is whether there is a different, special procedure for imprisonment of a citizen accused of wrongdoing *by aiding the enemy in wartime*." (emphasis in the original). *Id*. at 558 (Scalia, J., dissenting) (emphasis in the original).

53. *Id*. In *Hamdi*, three justices joined the O'Connor plurality for a total of four justices. Justice Souter filed an opinion concurring in part, dissenting in part, and concurring in the judgment, in which Justice Ginsberg joined. Justice Scalia filed a dissenting opinion in which Justice Stevens joined. Justice Thomas filed a solo dissenting opinion.

Intelligence Surveillance Court (FISC) to allow trials in secret.[54] There is no reason to prefer adding jurisdiction of secret criminal trials to the FISC, as opposed to establishing secrecy procedures for any federal district court. In fact, there may be reason not to: although the FISC operates with admirable secrecy, it was not meant to conduct trials. Instead, it was designed to establish the existence of probable cause, based only upon the government's ex parte appearance. Mixing the probable cause determination with an adversarial trial could raise due process questions or impugn the impartiality of subsequent trials.

The more intelligence collection has to respond to the demands of the criminal system, the less efficient and effective the intelligence will be. And the more the criminal system acts in concert with intelligence community, the more likely it becomes that an intelligence source or method will be pulled into a prosecution, with undesirable results. With the pressing issue of terrorist detainees driving policy, are the civilian and military criminal law systems adequate to deal with stateless individuals who present a clear and present danger? The United States has started to develop rules to govern the treatment of terrorist detainees. The federal courts have given some guidance, but rules reflecting a public or even judicial consensus are still inchoate. The most important policy issue in this area is how to reconcile two widely diverging approaches to a single target.

One possibility is to establish a rule of federal criminal procedure that would allow the trial judge to impose secrecy upon the process in ways that protect intelligence equities but allow both the prosecution and the defense to put on their cases without extra limitations. The CIPA already has a number of tools that can be used to that effect. It could be expanded to allow nonpublic trials, protective secrecy orders that applied to jury members, criminal sanctions for unauthorized disclosure of classified information introduced in evidence, and other means of confining national security information to the fewest necessary participants in a trial process. It is unlikely, however, that the news media or criminal defense interest groups would agree to such a new rule. The alternative to a new rule applicable by all federal district courts would be the creation of a new type of secret court itself, or the expansion of an existing one, where trials could play out without disclosure of anything but the outcome.

Regardless of the adjustments made to this boundary, no interest group will be entirely satisfied with the results. Again, the history of this boundary is perpetual adjustment to meet the necessities of the time.

54. Charlie Savage, *Push On to Clarify Rights for Detainees*, BOSTON GLOBE, May 31, 2005, at A1.

YOU WANT TO DO WHAT?!

The criminal law system also has a direct and significant effect on the ability of the intelligence establishment to conduct particular activities. In some public commentary and popular opinion, a magic and secret principle of law exempts intelligence agencies from substantive criminal prohibitions. Such an exemption would make the job of legal counsel to such agencies a great deal easier. But it does not exist. Intelligence activities that might implicate a U.S. criminal law must be reviewed on a case-by-case basis.

The intelligence community agencies, and especially the CIA, have special authorities that allow them to lawfully conduct activities that could be unlawful if conducted by other federal agencies or private individuals or organizations. Much of the authority granted to intelligence agencies is based upon the need for secrecy and the fact that most intelligence activities are directed at foreign governments, organizations, and individuals. But the latitude for action is limited when a specific criminal prohibition applies. For example, in the current Executive Order covering the intelligence community, section 2.8 provides: "*Consistency With Other Laws*. Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States."[55]

Some U.S. criminal statutes are so broadly worded that a specific exemption has been explicitly included to prevent otherwise authorized intelligence activities from being at least arguably covered by the prohibition. For example, 18 U.S.C. § 2511 makes it a crime to intercept electronic communications. Since intercepting electronic communications is the basic function of signals intelligence (SIGINT), a large portion of the intelligence community would be covered. In subsections 2511(2)(e) and (f), however, the drafters exempted electronic surveillance within the United States that is covered by FISA, as well as the acquisition of foreign intelligence information from international or foreign communications.[56]

Cybercrime, in the form of fraud and related actions in connection with unauthorized access or damage to computer systems, also contains a specific intelligence and law enforcement exemption.[57] Other statutes are broadly worded but not extraterritorial in application. Activities conducted abroad that do not involve U.S. persons or property or have a sufficient nexus with the territory of the United States may not be crimes.[58]

Other criminal statutes, however, are in fact clearly intended to apply to the activities of the U.S. government. For example, if possession of a biological or chemical weapon did not fall within the exceptions in the criminal statutes

55. Exec. Order No. 12,333 § 2.8, 46 Fed. Reg. 59,941, 59,952 (Dec. 4, 1981).

56. 18 U.S.C. §§ 2511(2)(e)-(f) (2005).

57. 18 U.S.C. § 1030(f) (2005).

58. *E.g.*, 18 U.S.C. § 231 (2005) (furthering civil disorders); 18 U.S.C. § 700 (2005) (desecrating the U.S. flag); 18 U.S.C. § 1001 (2005) (making false statements).

implementing the Biological and Chemical Weapons Conventions (relating to the purpose of the possession), intelligence agencies would be violating the law.[59] The federal crime of torture specifically refers to persons "acting under the color of law," meaning those acting on behalf of an official governmental entity. Torture is an extraterritorial federal crime and may not be authorized by any federal intelligence, military, or law enforcement official.[60] Period.

It is also clear that the President's authority to conduct covert actions is bounded by criminal prohibitions. In Title V of the National Security Act of 1947, as amended, the President is required to issue a finding authorizing any covert action. Title V goes on to state, "[a] finding may not authorize any action that would violate the Constitution or any statute of the United States."[61]

Unclear language in some criminal statutes and new circumstances that have expanded the reach of others create problems for intelligence agencies and their employees, however. In some statutes there is neither a specific exemption for otherwise authorized intelligence activities nor a clear intent to extend the law to cover such activities. For example, wire and mail fraud statutes state that "whoever" obtains money or property by means of false representations and uses the mail, telephone, radio, or television to do so, will be committing a federal crime.[62] There is no specific exclusion for otherwise lawful and authorized intelligence activities, and "whoever" seems all-inclusive on its face. If defrauding includes acquiring secrets of foreign persons and organizations by subterfuge or deceit, intelligence activities might be arguably included. That would be absurd in light of U.S. intelligence needs.

Another example is the criminal statute concerning provision of support to terrorists or terrorist groups.[63] Section 303 of the Antiterrorism and Effective Death Penalty Act, entitled "Prohibition on Terrorist Fundraising" subjects to criminal prosecution, "whoever knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so."[64] There is no intelligence exception in the text of the statute. There is no discussion of intelligence activities in the legislative history. There is no explicit expression of congressional intent to include or exclude intelligence activities from the reach of the prohibition.

On its face, the language would cover an intelligence agency and its employees who provide money or equipment to assist a human asset in establishing his bona fides in order to penetrate a terrorist organization. Interpretation of the statutory language in that way could create a bizarre result. Precluding the federal government itself from taking steps to fight international

59. 18 U.S.C. §§ 175(c), 229F(7) (2005).

60. 18 U.S.C. §§ 2340- 2340A (2005).

61. 50 U.S.C. § 413b(a)(5) (2005).

62. 18 U.S.C. §§ 1341, 1343 (2005).

63. Antiterrorism and Effective Death Penalty Act, Pub. L. No. 104-132, 110 Stat. 1214 (codified in scattered sections of the U.S.C.).

64. 18 U.S.C. § 2339B (2005).

terrorism would defy both logic and the statutory purposes expressed in report language. Providing material support to a terrorist organization in order to penetrate and defeat it brings the intelligence world—where all is not as it seems in many circumstances—into conflict with a criminal law system that is premised upon constitutional requirements of clarity, proof beyond a reasonable doubt, and lines between right and wrong.

There are other examples. Intelligence agencies deploy officers and assets in the field under various types of cover. Cover protects their personal safety and their affiliation with the United States. It sometimes requires ruses and false-flag persona. Yet, "[w]hoever falsely and willfully represents himself to be a citizen of the United States shall be fined under this title or imprisoned not more than three years, or both."[65] Such an act is a felony. There is no exception for intelligence activities. According to the bare statutory text, a non-U.S. citizen working for the CIA thus cannot say that he is a U.S. citizen to anyone who is a potential intelligence source. Should CIA officers pretend to be "associated with" 4-H clubs (as far-fetched as that might be) they could also violate 18 U.S.C. § 916, a statute that bans holding oneself out falsely as a member or representative for that group. And so on.

In such cases, principles of statutory interpretation are the only way to reconcile statutory intent with statutory language. The most important is the *Nardone* rule, which states that criminal laws of general applicability should not be interpreted to apply to actions of the government as sovereign unless there is specific language to that effect.[66] Other rules of interpretation also require looking to the reasons for enactment of the statute and the purpose to be gained by it, and construing the statute in the manner which is consistent with such purpose. A statute should not be read literally where such a reading is contrary to its purposes.[67]

The difficulty with reliance on such rules is that *Nardone* is not sweeping in reach and each case requires an examination of the particular facts. Subjecting intelligence activities to advance legal review for potential criminal activities, and producing the resulting legal opinions in coordination with the Department of Justice, is time consuming, inefficient, and unfair to those intelligence officers at risk of being targets of criminal investigations.

It is unlikely that such officers would ultimately be convicted for actions they believed to be officially authorized. For one reason, they would not possess the required mens rea, or criminal intent, in almost every situation.

65. 18 U.S.C. § 911 (2005).

66. "The second class, [of cases in which the canon that the general words of a statute do not include the government unless the construction of the text is clear and indisputable]—that where public officers are impliedly excluded from language embracing all persons,—is where a reading which would include such officers would work obvious absurdity as, for example, the application of a speed law to a policeman pursuing a criminal or the driver of a fire engine responding to an alarm." Nardone v. United States, 302 U.S. 379, 384 (1937).

67. NORMAN J. SINGER, SUTHERLAND STATUTORY CONSTRUCTION § 46.07 (5th ed. 1992).

That would be a defense to criminal charges which is based upon actual or believed exercise of public authority. This defense has been explicitly recognized in FRCrP 12.3, which requires notice to the prosecution and disclosure of witnesses when it is raised.

For another, intelligence activities are reviewed by Agency legal counsel. Agency employees proceed at their own peril when they carry out activities over the objections of Agency counsel that are based upon possibly criminal liability. Yet in grey areas, employees could be subject to criminal investigations for actions taken under the stress, danger, and critical time pressures experienced in the field. A criminal investigation has highly serious effects upon individuals and organizations, even if—after years go by—no charges or other sanctions are ever brought.

So-called "dirty" assets raise the same issues. Sources of certain intelligence information may be individuals who have committed crimes under U.S. law even though their actions took place completely overseas. This is most likely in areas such as terrorism, narcotics trafficking, and weapons proliferation. The criminal law system wants to convict them or use them to convict others. Intelligence wants to use them to collect information that will remain secret. Continuing to use human assets to collect intelligence after information surfaces tying them to a crime significantly increases the likelihood that a successful criminal case cannot be brought against them without seriously risking intelligence equities. In such a case, it is not impossible to serve both intelligence and criminal interests, but it is very difficult.

At a minimum, the least intelligence officers should expect is clarity and predictability in the criminal laws. The Department of Justice could always subject extreme cases to a review for the purpose of declining prosecution if appropriate. Such reviews, however, are painstaking and highly dependent upon, and restricted to, individual facts and circumstances. In grey areas, using review procedures is not a useful way to establish criminal law boundaries to otherwise lawful and authorized intelligence activities.

These concerns were reflected in Title XI of the National Security Act, which was added to create a statutory interpretation presumption that U.S. domestic laws implementing international treaties and conventions would not make unlawful otherwise lawful and authorized intelligence activities, absent express statutory language to the contrary.[68] Title XI recognizes that it would be exceedingly difficult for the Departments of State and Justice to ensure that every new transnational criminal convention and its implementing legislation contain a specific exemption for intelligence activities. Trying to address issues of espionage, covert action, and other unacknowledged national state activities in an international convention would be next to impossible. Public discussion necessary to adopt such agreements would be very damaging to the clandestine activities that the agreements sought to protect. As a result, it was necessary to

68. 50 U.S.C. § 442 (2005).

craft this rule of statutory interpretation to make Congressional intent manifest when it otherwise was silent.

The secrecy in which intelligence agencies operate is not a shield either. Section 1.7 of Executive Order 12,333 (signed in 1981) has required all components of the intelligence community to report possible violations of federal criminal laws by employees, and specified federal criminal laws by any other persons, under procedures developed between the Attorney General and the intelligence organization involved.[69]

In 1982, then-Attorney General William French Smith and then-Director of Central Intelligence William Casey signed such guidelines for the CIA. In brief, they require the General Counsel (currently a Senate-confirmed presidential appointment) to report to the Criminal Division of the Department of Justice and the FBI any basis that an Agency employee may have violated any federal crime, and any basis that any person may have committed any of a list of serious federal offenses such as those involving intentional infliction or threat of death or serious physical harm, espionage, or perjury or false statements. Crime reporting is extensive, and significant effort is devoted to it. In addition, in the late 1980s Congress created a statutory Inspector General for the CIA. The Inspector General's duties include investigating possible violations of federal criminal laws that involve programs or operations of the Agency, and reporting any such information to the Attorney General.[70]

The criminal law system can be a profound deterrent to intelligence activities. Criminal law can be a bar to actions of even the President of the United States. It is unlikely that government employees will be found guilty of a crime if they are carrying out in good faith what is otherwise a lawful activity. But subjecting those individuals responsible for implementing U.S. foreign policy and national security policy to criminal investigations, even when no charges are ever brought, can be a punishing and debilitating experience for both the individuals and their agencies, often lasting years in duration.

From the perspective of those executing the laws, criminal offenses should be clearly written and widely understood by all. Legislating specific exemptions for intelligence activities on a bill-by-bill basis exposes intelligence practices and establishes at least the argument that without a specific exemption, Congress means to make a crime out of an otherwise lawful U.S. government action. In other circumstances, where Congressional intent in creating a particular crime is either deliberately or inadvertently vague, the Criminal Division of the Department of Justice will be forced to painstakingly review in advance every proposed intelligence activity in areas where no agreement can be reached on whether such activities are exempt. No intelligence service can operate effectively that way. Intelligence agencies will simply avoid potential sources, methods, and activities that raise such a risk.

69. Exec. Order No. 12,333 § 1.7, 46 Fed. Reg. 59,941, 59,945 (Dec. 4, 1981).

70. Central Intelligence Agency Act of 1949 § 17, 50 U.S.C. § 403q(b)(5) (2005).

One suggestion has been made to enact a *Nardone*-like presumption of statutory interpretation that a particular criminal statute should not be deemed to apply to otherwise lawful and authorized intelligence activities unless the text explicitly directed that it should be. The presumption could be overcome by simply including language in the particular criminal statute to the effect that it does apply to intelligence activities. Unauthorized, *ultra vires* actions by individuals who were not conducting officially approved activities would remain crimes under any law that applied. A non-statutory alternative would be to establish as Executive Branch policy a presumption based upon the *Nardone* rule. That could be done by executive order, presidential decision directive, or Attorney General policy decision. Such a policy could have the advantage of being strongly rooted in Constitutional notions of separation of powers that leave near-complete discretion over decisions to prosecute to the Executive Branch.

The criminal law system thus directly affects intelligence authorities and officers and employees who carry out intelligence activities. Both the substantive criminal law and the organizations that enforce it are integral parts of the arena in which the intelligence community operates. There is no "get out of jail free" card.

As policymakers deal with the numerous recent suggestions for reorganizing and bettering the intelligence community, they should remember one principle: information that surfaces indicating that a crime has been committed by individuals associated with that community will bring everything nearby, including vital and lawful intelligence collection efforts, to a screeching halt.

CONCLUSION

All three of the discussed areas affect the others. The breakdown of the wall brings more intelligence information into the realm of criminal procedure. Expansion of crimes overseas as a result of the convergence of targets will restrict actions of the intelligence community. Prosecutions will be put at risk when intelligence equities arise.

There is a current laboratory in which these factors are colliding. The United States has recently embarked upon a significant and far-reaching reorganization of the executive branch agencies that deal with threats. The creation of new entities such as the Department of Homeland Security, the National Counterterrorism Center, and the National Counterproliferation Center has forced together those responsible for carrying out criminal laws and intelligence laws. The laws themselves are being rewritten to take into account the new overlaps.

The main purposes of ordinary criminal law are to punish wrongdoers and deter others from doing wrong. The concept of justice illuminates everything involved in it. While intelligence may serve justice, its purposes are far

different. Conflict in mission, resources, authorities, and responsibilities is inevitable among the diverse government components that execute criminal justice and intelligence laws. At some point, compromises to solve those conflicts by meeting the needs of both systems may degrade both systems beyond what is acceptable. At such a point, someone will have to win and someone will have to lose. As the new system of government organizations is established to meet threats (which includes both criminal law and intelligence aspects), an efficient process by which such conflicts are resolved is as important as the substance of the conflicts themselves.

The federal judiciary has shown a highly important ability and willingness to craft accommodations between the two legal regimes. However, judges are limited by jurisdiction. They address disputes that arrive before them, and precedent can influence similar cases in the future. But a case remains at best an unsound way to bring criminal law and intelligence systems jointly to bear on a particular target. Employees and contractors of the federal government should not have to resort to the courts to reconcile competing legal equities of criminal law and intelligence, unless some fundamental principle of justice is involved.

America has historically put a great deal of faith in the criminal law as a means to solve a problem or meet a threat. Nevertheless, terrorism, narcotics, and driving while intoxicated have aspects that keep them far beyond the ability of the criminal law system alone to solve. Adjustments at the borders, rather than new physics, may continue to be the most likely way to accommodate most, but never all, of the goals of each system. For example, closed trials may greatly offend the news media but in some cases could meet both the need to protect intelligence sources and methods and the need for a fair trial. Federal courts could adopt special procedures for discovery, trial, and sentencing in national security crimes.[71] Additional procedural safeguards could be imposed on the use in a criminal trial of information obtained on the basis of intelligence authorities and techniques. A principle of statutory interpretation could be adopted to further clarify criminal laws that might prohibit otherwise lawful intelligence activities.

Still, perfection in either realm is beyond reach. As has always been the case, the ultimate success of managing the missions will depend on the skill of the attorneys, the sophistication of the courts, and the tolerance of ambiguity by the American public.

71. *E.g.*, those crimes that are likely to have national security or intelligence implications by the nature of the crimes themselves, such as those included in 18 U.S.C. § 2 (aircraft hijacking and piracy); § 10 (biological weapons); § 11B (chemical weapons); § 37 (espionage); § 50A (genocide); § 105 (sabotage); § 113B (terrorism); § 115 (treason); and § 118 (war crimes).