Extraterritorial Issues

In This Issue

March 2007 Volume 55 Number 2

United States Department of Justice Executive Office for United States Attorneys Washington, DC 20530

Steven J. Parent Acting Director

Contributors' opinions and statements should not be considered an endorsement by EOUSA for any policy, program, or service.

The United States Attorneys' Bulletin is published pursuant to 28 CFR § 0.22(b).

The United States Attorneys' Bulletin is published bimonthly by the Executive Office for United States Attorneys, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201.

Managing Editor Jim Donovan

Program Manager Nancy Bowman

Law Clerk Kevin Hardy

Internet Address www.usdoj.gov/usao/reading_room/foiamanuals.html

Send article submissions and address changes to Program Manager, United States Attorneys' Bulletin, National Advocacy Center, Office of Legal Education, 1620 Pendleton Street, Columbia, SC 29201.

In Honor

This issue of the United States Attorneys' Bulletin is dedicated to Michael T. Shelby, the former United States Attorney for the Southern District of Texas. Mr. Shelby served as an Assistant United States Attorney for over ten years and as United States Attorney from 2002 to 2005.

As a career prosecutor, Michael worked for five years as an Assistant District Attorney at the Harris County District Attorney's Office, serving primarily in the Special Prosecutions Division. In 1989, he joined the United States Attorney's Office in Houston, as an Assistant United States Attorney, specializing in the investigation and prosecution of cases involving public corruption, organized crime, and environmental law. In 1997, he moved to Phoenix, Arizona, where he continued his work as an Assistant United States Attorney, prosecuting corrupt public officials. In early spring 2002, Michael was sworn in as the United States Attorney for the Southern District of Texas. Among his many accomplishments while serving as the United States Attorney, was his creation of the Anti-Terrorism Advisory Council, which was used nationwide as the model for other United States Attorneys' offices.

Michael was a Commissioned Officer in the U.S. Naval Reserve, where he held the rank of Commander (Select) and was assigned to Reserve SEAL Team FIVE. He was a decorated veteran with active military service in the Middle East during Operation Desert Storm, and in Bosnia.

Michael was the recipient of the Executive Office for United States Attorneys' Director's Award and received numerous awards from the Federal Bureau of Investigation (FBI), the U.S. Drug Enforcement Administration (DEA), the U.S. Customs Service, the Environmental Protection Agency, the Internal Revenue Service, the National Aeronautics and Space Administration, and numerous state and local law enforcement agencies. He received personal letters of commendation from Attorney General Janet Reno and FBI Directors Louis Freeh and William Sessions. He routinely served as an instructor for the FBI, DEA, and the Department's National Advocacy Center, where he taught Basic Trial skills to fellow prosecutors. In recognition of his commitment as a prosecutor and teacher, Courtroom A106 at the National Advocacy Center was dedicated in his honor.

Michael passed away on July 18, 2006, after a courageous battle with cancer. He was a man of strength, humor, integrity and great love. He believed that the greatest gift in life is time, and he was an example to all who knew him of living his life to the fullest. He was an expert sky diver, snow and water skier, mountain climber, marathon runner, as well as an award winning screenplay writer.

He is survived by his wife, Diana Jane Shelby; two daughters, Elizabeth Jane Shelby and Sarah Seay Shelby; his mother, Marilyn Seay Shelby; two brothers, Robert Seay Shelby, and David Shelby, Jr.; and two sisters, Teena and Lisa Shelby. He will be remembered by his family, friends, and colleagues, for his firm commitment to his profession and his exemplary service to his country as an Assistant United States Attorney, United States Attorney, and as a member of the Navy's elite SEAL Team FIVE.

Fundamental Principles Governing Extraterritorial Prosecutions– Jurisdiction and Venue

John De Pue
Senior Trial Attorney
Counterterrorism Section
National Security Division

I. Introduction

The purpose of this issue of *United States Attorneys' Bulletin* is to address legal principles governing matters that frequently arise in the prosecution of extraterritorial terrorism cases. These include the ability of the United States to proscribe such acts and assert jurisdiction over them, the determination of the district in which such prosecutions will be venued, and the ability of the United States to project its investigative and law enforcement capabilities overseas. Although the principles contained in this survey represent the current views of the Counterterrorism Section and comport with what the Department of Justice (Department) believes to be the present state of the law, just as in any criminal prosecution, government counsel should always consult the current law of the circuit and its application to the particular case. Should legal issues arise that require further guidance, it may be obtained from either the Criminal Division's Counterterrorism Section or the Department's Office of Legal Counsel.

II. Jurisdiction

A. Definitions

Jurisdiction in a criminal case addresses power or authority—the question of jurisdiction informs prosecutors of both the authority by which Congress enacts legislation and the authority that the courts have to act in a particular case.

In contrast, the term venue simply defines the judicial district in which such authority is to be exercised, once an offense is committed.

B. Constraints under international law—limitations on the exercise of jurisdiction when such action infringes upon the rights of other sovereigns

Extraterritorial jurisdiction simply relates to the authority of a government to criminalize activity that occurs outside its territorial borders, or to investigate or prosecute such activity. The exercise of extraterritorial jurisdiction by one state with respect to criminal activity necessarily encroaches, in some measure, upon the sovereignty of the nation where the offense occurred. Under customary international law, there are five generally recognized principles upon which a country can permissibly assert extraterritorial jurisdiction. *See United States v. Yousef*, 327 F.3d 56, 91-92 (2d Cir. 2003). The jurisdictional bases include the following.

- The objective territorial principle—where the offense occurs in one country but has effects in another, for example, killing someone by shooting across an international border.
- The nationality principle—the offender is a citizen of the prosecuting state.
- The protective principle—the offense offends the vital interests of the prosecuting state, such as counterfeiting that nation's currency.
- The passive personality principle—the victim is a citizen of the prosecuting state.
- The universality principle—the offense, such as piracy, is universally condemned by the international community, sometimes in a multinational convention or treaty to which the United States is a signatory.

Furthermore, in *Yousef*, the court held that, where a jurisdictional provision authorizing its extraterritorial assertion has been enacted to implement a treaty obligation, the relevant treaty provision is, itself, a sufficient basis under international law for asserting such jurisdiction.

Despite these limitations upon the exercise of extraterritorial jurisdiction stemming from customary international law, where Congress has clearly articulated its intent to legislate extraterritorially, the legislation trumps any limitation upon the assertion of such jurisdiction based upon customary international law. *Id* at 327; *United States v. Yunis*, 924 F.2d 1086, 1091 (D.C. Cir. 1991). However, where Congress's intent is silent, the courts ordinarily infer that it intended to legislate in a manner that is in harmony with such principles.

C. Constitutional constraints upon the assertion of extraterritorial jurisdiction

Several circuits have held that, where Congress criminalizes extraterritorial conduct, substantive due process requires some nexus between the United States, or its vital interests, and the proscription. *Yousef*, 327 F.3d at 112 (plan to attack Philippine Airlines flight sufficiently related, under Due Process Clause, to U.S. interests, where attack was a "test run" for further attacks on U.S. flag carriers); *United States v. Davis*, 905 F.2d 245 (9th Cir. 1990) (finding adequate nexus to U.S. interests where facts showed that defendant intended to smuggle drugs into U.S. territory); *see also United States v. Clark*, 435 F.3d 1100, 1108 (9th Cir., 2006) (defendant's U.S. citizenship sufficient to satisfy due process concerns); *but cf. United States v. Martinez-Hidalgo*, 993 F.2d 1052 (3d Cir. 1993) (no nexus with the United States required where the extraterritorial conduct is universally condemned by law-abiding nations). The Due Process Clause is ordinarily satisfied merely by demonstrating that the offense falls within one of the five internationally recognized bases for asserting extraterritorial jurisdiction set out above. *Cf. United States v. Marino-Garcia*, 679 F.2d 1373, 1379-81 (11th Cir. 1982) (imputing to Congress the intent to confine reach of extraterritorial jurisdiction over a stateless vessel on the high seas to that permitted under international law).

Congressional authority to legislate extraterritorially does not, by itself, create extraterritorial jurisdiction. Congress must enact a statute authorizing the assertion of such jurisdiction, and it is clear that it possesses the power under the Constitution to do so. *See EEOC v. Arabian Amer. Oil Co.*, 499 U.S. 244, 248 (1991).

Nonetheless, Congress is not ordinarily held to the same standard, in relation to explicit Constitutional authority, when legislating extraterritorially as it is in the enactment of domestic legislation. This is because extraterritorial legislation does not possess the same capacity to encroach upon governmental powers reserved to the states and because the United States has the inherent sovereign power to legislate extraterritorially. *See United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 315 (1936); *see also Japan Line, Ltd, v. County of Los Angeles*, 441 U.S. 434, 448 (1979).

In this respect, Constitutional bases for the enactment of extraterritorial legislation include the following.

- An incident of the Congressional authority to "Define and punish offenses against the law of nations." U.S. Const. Art. 1 § 8, cl. 8.
- An incident of Congressional authority to implement treaties under the "necessary and proper clause" of Article I § 8, cl. 18.
- An incident of Congressional authority "to regulate Commerce with foreign Nations." Art. I § 8, cl.3. *See United States v. Clark*, 435 F.3d at 1114-17 (approving legislation prohibiting travel in foreign commerce to engage in illicit sexual activities with minors).

D. Determining whether a statute is intended by Congress to be extraterritorial

Under both international law and the Constitution, Congress possesses the authority to legislate extraterritorially. Nevertheless, it is necessary to inquire whether, in the context of a particular statute, it has, in fact, done so. First, consider the language of the statute. Does it expressly address its jurisdictional scope? Statutes that contain formulas specifically defining the scope of jurisdiction include the following.

- Foreign murder of a U.S. national (18 U.S.C. § 1119).
- War crimes (18 U.S.C. § 2441).
- Murder of, or assault upon, a U.S. national abroad for the purpose of coercion, intimidation, or retaliation, as certified by the Attorney General (18 U.S.C. § 2332).
- Use of weapons of mass destruction (18 U.S.C. § 2332a).

- Bombing public places or facilities (18 U.S.C. § 2332f (b)).
- Providing material support to foreign terrorist organizations (18 U.S.C. § 2339B(d)).
- The commission of certain felony offenses by persons accompanying the armed forces overseas (18 U.S.C. § 3261).

Some federal statutes are expressly confined in their application to the "special maritime and territorial jurisdiction of the United States," for example, murder under 18 U.S.C. § 1111. The phrase "special maritime and territorial jurisdiction" is defined in 18 U.S.C. § 7. It includes federal enclaves, such as the following.

- National parks and military installations.
- Territorial waters.
- U.S. flag vessels.
- U.S.-owned aircraft (while flying in U.S. airspace, or over international waters).

It also includes some territory outside the United States, such as the following.

- Places not subject to the jurisdiction of any nation with respect to crimes by or against U.S. nationals. *See* 18 U.S.C. § 7(7).
- The premises of U.S. diplomatic, consular, military, or other U.S. missions or entities in foreign states or residences relating to such entities (but only when the victim or the offender is a U.S. national). *See* 18 U.S.C. § 7(9).

Thus, in some instances, an offense committed within the "special territorial jurisdiction of the United States" may actually involve an extraterritorial crime. Finally, some statutes reach criminal activity involving "any building, vehicle, or other real or personal property in whole or in part owned or possessed by, or leased to the United States or any department or agency thereof . . . ." *See* 18 U.S.C. § 844(f)(1); 18 U.S.C. § 2252A(a)(4)(A). Such broad language can also reasonably be construed to reach such property and facilities of the United States even when outside the territorial limits of the United States. *But see United States v. Martinelli*, 62 M.J. 52, 60 (C.A.A.F. 2005) (three members of Court of Appeals for the Armed Forces holding that such language is not extraterritorial).

"Special aircraft jurisdiction" is another jurisdictional term of art that governs aircraft piracy (49 U.S.C. § 46502) and the statute proscribing the destruction of an aircraft (18 U.S.C. § 32). The term is defined in 49 U.S.C. § 46501(2). To be cognizable under the air piracy statute, an offense must be committed while the aircraft is "in flight," a term of art defined in 49 U.S.C. § 46501(1).

E. Jurisdictional provisions common to statutes implementing treaties

The United States is party to a number of multilateral agreements designed to combat terrorism. These agreements contain provisions requiring signatories to criminalize the proscribed conduct and either extradite or prosecute persons present within their territory who are believed to have committed prohibited acts. Statutes implementing such treaties, therefore, authorize prosecution of any offender by virtue of his mere presence in the United States. Hostage taking (18 U.S.C. § 1203) is an example of an offense upon which extraterritorial jurisdiction can be predicated solely upon the defendant's being "thereafter found" in the United States. The phrase "thereafter found" has been held to include the defendant's forcible rendition for the purpose of standing trial for another offense (*see Yunis*, 924 F. 2d at 1090) or for the very crime to which the "thereafter found" provision applies. *See United States v. Rezaq*, 134 F.3d 1121 (D.C. Cir. 1998) ("afterward found" requirement permits prosecution for aircraft piracy even in cases where defendant is forcibly returned to the United States to stand trial for only that offense). A number of multilateral agreements designed to combat terrorism, the implementing federal legislation, and jurisdictional provisions of such legislation, are provided as an addendum to this article.

F. What if the statute is silent with respect to its extraterritorial application?

The presumption of territoriality. As the Supreme Court recently observed in *Small v. United States*, 544 U.S. 385, 388-89 (2005), "in determining the scope of [a] statutory phrase, we find help in the commonsense notion that Congress generally legislates with domestic concerns in mind. . . . This notion has led the Court to adopt the legal presumption that Congress ordinarily intends its statutes to have domestic, not extraterritorial application." *Id.* (citation and internal quotes omitted). For example, crimes against individuals or their

property, such as assaults, murder, burglary, larceny, robbery, and other offenses which affect the peace and good order of the community are, unless Congress expressly says to the contrary, presumptively territorial in scope. *United States v. Bowman*, 260 U.S. 94, 98 (1922).

A statute does not, however, become extraterritorial, so as to require an assessment as to whether Congress intended to override the presumption of territoriality, simply because the legislation reaches activities that occur (or are intended to occur) outside the territorial jurisdiction of the United States. Thus, such an offense can be considered a domestic crime if a portion of the crime occurred in the United States. *See United States v. Moncini*, 882 F.2d 401, 402 (9th Cir. 1989) (introducing child pornography into the United States through the mails); *see also United States v. Lombardo*, 241 U.S. 73, 77 (1916) ("where crimes consist of distinct parts which have different localities the whole may be tried where any part can be proved to have been done"); 18 U.S.C. § 3237 (any offense involving the use of the mails or transportation in interstate or foreign commerce, is a continuing offense and may be prosecuted in any district through which subject matter moves).

In *Pasquatino v. United States*, 544 U.S. 349 (2005), the Supreme Court rejected the argument that the government had improperly employed the federal wire fraud statute (18 U.S.C. § 1343), which prohibits the use of interstate wires to effect "any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses," to reach extraterritorial conduct—the smuggling of untaxed liquor into Canada. Expressly addressing concerns articulated in Justice Ginsburg's dissent that the use of the statute for such a purpose would contravene the presumption of extraterritoriality, *Id*. at 377 (Ginsburg, J., dissenting)), the Court reasoned:

> [O]ur interpretation of the wire fraud statute does not give it 'extraterritorial effect.' . . . Th[e] [defendant's] offense was complete the moment they executed the scheme inside the United States; '[t]he wire fraud statute punishes the scheme, not its success.' . . . This domestic element of petitioner's conduct is what the Government is punishing in this prosecution, no less than when it prosecutes a scheme to defraud a foreign individual or corporation, or a foreign government acting as a market participant.

Id. at 371. Thus, by the same token, where the locus of a conspiracy to provide material support to a foreign terrorist organization (18 U.S.C. § 2339(b)) is within the jurisdiction of the United States, the offense does not become extraterritorial simply because the material support is destined for a beneficiary that engages in extraterritorial terrorist activities. In such cases, it is unnecessary to consider whether Congress expressly intended to reach extraterritorial activity, as the offense is territorial in nature.

The exception that largely swallows the rule. The *Bowman* Court made it clear that the "presumption of territoriality" has no application with respect to legislation that does not simply codify common law breaches of the peace and is designed to deter injury to the United States and its interests, regardless of the locus of the offense. The Court explained as follows.

> [T]he same rule of interpretation [*i.e.*, the presumption of territoriality] should not be applied to criminal statutes which are, as a class, not logically dependant upon their locality for the government's jurisdiction, but are enacted because of the right of the government to defend itself against obstruction or fraud wherever perpetrated, especially if committed by its own citizens, officers or agents. . . . [T]o limit their *locus* to the strictly territorial jurisdiction would be to greatly curtail the scope and usefulness of the statute and leave open a large immunity for frauds as easily committed by citizens on the high seas, and in foreign countries as at home. In such cases, Congress has not thought it necessary to make specific provision in the law that the locus shall include the high seas and foreign countries, but allows it to be inferred from the nature of the offense.

Bowman, 260 U.S. at 98.

Relying upon this language, the courts of appeals have repeatedly viewed federal statutes, otherwise silent as to their jurisdiction application, to involve subject matter from which it could be inferred that Congress intended extraterritorial application. Examples of offenses where Congressional intent to trump the presumption of

territoriality has been inferred include the following.

- Fraud or making false claims against the government (*Bowman*, 260 U.S. at 99-100).
- Conspiracy to induce aliens to unlawfully enter the United States (*United States v. Delgardo-Garcia*, 374 F.3d 1337, 1346 (D.C. Cir. 2004)).
- Extraterritorial conspiracy to bomb U.S. registered aircraft (United States v. Yousef, 327 F.3d at 87-88).
- Smuggling contraband into the United States (*United States v. Plummer*, 221 F.3d 1298 (11th Cir. 2000)).
- Conspiracy to import narcotics into the United States (*United States v. McAllister*, 160 F.3d 1304, 1308-09 (11th Cir. 1998) (collecting cases)).
- Conspiracy to murder and assault a U.S. government official (*United States v. Benitz*, 741 F.2d 1312 (11th Cir. 1984)).

But see Small v. United States, 544 U.S. 385, 387 (2005) (invoking presumption of territoriality and holding that offense of possession of a firearm by a convicted felon does not apply to foreign convictions); *United States v. Martinelli*, 62 M.J. 52 (narrowly construing exception to presumption of territoriality to apply only to frauds against government and holding that presumption applies to receipt of child pornography).

Finally, in determining whether Congress intended that a statute apply outside the borders of the United States, it is appropriate to take into account not only its purpose, but also its structure, legislative history, and, in appropriate cases, the text and negotiating history of the treaty which the legislation implements. *See Sale v. Haitian Ctrs. Council*, 509 U.S. 155, 174-77 (1993) (examining legislative history of statute, as well as text and history of the convention it implemented, to determine whether "forced repatriation" provisions of the Immigration and Nationality Act were intended to apply extraterritorially).

Offenses that are ancillary to extraterritorial crime. Attempts, accessory after the fact, conspiracy, and the use of a firearm during and in relation to a crime of violence (18 U.S.C. § 924(c)), have been held to assume the territorial character of the base offense. *See Yousef*, 327 F.3d at 87-88 (collecting cases); *United States v. Lindh*, 212 F. Supp. 2d 541, 580 (E.D. Va. 2002) (an extraterritorial violation of 18 U.S.C. § 2339B is a crime of violence to which a § 924(c) use of a firearms count can attach); *see also United States v. Khan*, 309 F. Supp. 2d 789, 823 (E.D. Va., 2004); *United States v. Goba*, 240 F. Supp. 2d 242, 249 (W.D.N.Y. 2003). Thus, it is unnecessary to conduct a separate inquiry as to whether Congress intended such an ancillary offense to have extraterritorial effect.

G. Prohibitions against "providing material support"

Title 18 U.S.C. §§ 2339A and 2339B, respectively, prohibit providing "material support or resources" knowing or intending that they are to be used in preparation for, or carrying out, one of a number of enumerated terrorist crimes (§ 2339A) or knowingly providing "material support or resources" to a foreign terrorist organization (FTO) (§ 2339B). Both statutes embrace attempts and conspiracies as well. Since the events of September 11, 2001, these two statutes have become mainstays in the Department's war on terrorism. As of April 2005, eighty-nine persons have been charged with violations in sixteen different districts. In addition, § 2339C, which is discussed in connection with the Terrorist Financing Convention, *infra,* prohibits providing or collecting funds to foster acts of terrorism.

Section 2339A. As originally enacted, 18 U.S.C. § 2339A prohibited a person "within the United States" from providing material support or resources, knowing that it would be used for the commission of a terrorist crime. *See* Pub. L. No. 103-322 § 120005, 108 Stat. 2022 (1994). As part of the USA PATRIOT Act, however, the jurisdictional limitation, "within the United States," was deleted. Pub. L. No. 107-56, § 805, 115 Stat. 377 (2001). The plain implication of that amendment was to expand the jurisdictional scope of the statute to extraterritorial acts of providing material support. Thus, it would appear, at a minimum, that such offenses are now akin to "ancillary offenses," which means that their jurisdictional scope corresponds to that of the crime that the material support or resources is intended to facilitate. Consequently, after October 26, 2001, where the contemplated terrorism offense permits the exercise of extraterritorial jurisdiction, so also would a § 2339A violation designed or intended to facilitate it. Prior to that date, the prohibited conduct must have occurred

"within the United States" to constitute a violation of § 2339A.

Section 2339B. In contrast to § 2339A, as originally enacted, persons embraced by the prohibition against providing material support or resources to FTOs were limited to those "within the United States or subject to the jurisdiction of the United States." Subsection (d) stated that "[t]here is extraterritorial Federal jurisdiction over an offense under this section"—a provision that the Department believes was intended to make clear that the phrase "or subject to the jurisdiction of the United States" reached persons *outside* the United States who provided such material support to an FTO, as long as they were U.S. nationals. The scope of the jurisdictional predicate–subject to the jurisdiction of the United States–is not settled. At the least, the term embraces U.S. nationals and corporations. It is not certain whether it includes resident aliens as well.

As part of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (IRTPA), Congress substantially expanded the jurisdictional provisions of § 2339B. In particular, it authorized the assertion of jurisdiction over the provision of material support to an FTO under the following circumstances.

- The offense (the provision of material support or resources) occurred, in whole or in part, in the United States.
- The offender is a U.S. citizen or a permanent resident alien.
- The offender is a stateless person whose habitual residence is the United States.
- The offender is brought into or found in the United States, after the conduct for the offense occurred, even if the conduct required for the offense occurred outside the United States.
- The offense occurred in, or affects, interstate or foreign commerce.
- The offender aided and abetted or conspired with any person over whom jurisdiction exists under any of the above circumstances.

Thus, as amended by the IRTPA, in many instances where the predicate conduct—the provision of material support—neither occurs within the United States nor is perpetrated by a U.S. national, § 2239B permits the exercise of extraterritorial jurisdiction. Perhaps the most dramatic extension of extraterritorial jurisdiction involves instances where the defendant provides material support to an FTO overseas and is then prosecuted by virtue of his mere presence, whether voluntary or involuntary, in the United States. The justification for the assertion of such jurisdiction is that, by providing assistance to an FTO—which by definition presents a threat to the security of the United States—the defendant engages in conduct which, itself, threatens the security of the United States. This rationale is supported by the "protective" theory of extraterritorial jurisdiction that was discussed previously. The new jurisdictional provisions to § 2339B should not be employed, as the basis for asserting jurisdiction over an offense, where the prohibited conduct predated December 17, 2004, the date of IRTPA's enactment. An attempt to do so would implicate constitutional *Ex Post Facto* principles.

Section 2339C. As noted earlier, § 2339C, which became effective June 25, 2002, in the wake of the United States' accession to the Terrorist Financing Convention, prohibits fund-raising or monetary contributions to those bent upon undertaking activities that violate one of a number of international terrorism conventions. It also reaches contributions made with knowledge that the funds are to be used to carry out acts intended to cause death or bodily harm for the purpose of intimidating a population or compelling a government. The role of § 2339C will likely be confined to those rare instances where the jurisdictional provisions of §§ 2339A and 2339B do not reach a person located abroad, but against whom a U.S. prosecution is appropriate. Note the multiple jurisdictional predicates enumerated in § 2339C(b) and summarized in our compilation of treaty-implementing jurisdictional provisions. One of them permits the assertion of extraterritorial jurisdiction over an offense on the basis of the defendant's presence in the United States, alone.

Section 2339D. Section 2339D was added to Chapter 113 of Title 18 (of which §§ 2339A, B and C are also a part), by the IRTPA. Briefly summarized, § 2339D prohibits the receipt of military-type training from, or on behalf of, an FTO, with knowledge that the organization has been so designated or that it engages in terrorist activity. The jurisdictional predicates for this offense are virtually the same as for a violation of § 2339B discussed above. Therefore, there are a variety of bases for the assertion of extraterritorial

jurisdiction, including the fact of the defendant's subsequent presence in the United States, whether voluntary or involuntary.

III. Venue

A. Constitutional constraints

U.S. Const. Art. III, § 2, cl. 3 provides:

> All criminal trials, [except in cases of impeachment] shall be held in the State where such crime shall have been committed; but when not committed within any State, the trial shall be at such Place or Places as Congress may by law have directed.

The final phrase ("but when not committed . . . ") has been held to "impose no restriction as to the place of trial, except that the trial cannot occur until Congress designates the place, and may occur at any place which shall have been designated." *Cook v. United States*, 138 U.S. 157, 182 (1891).

B. Proof requirements

Venue must be established by a preponderance of the evidence. *See United States v. Naranjo*, 14 F.3d 145, 146 (2d Cir. 1994). Unlike claims based upon a lack of jurisdiction, however, claims of improper venue are waived if not raised prior to trial. *See Singer v. United States*, 380 U.S. 24 (1965). Charging papers should allege the basis for venue in the particular district.

C. Venue statutes for territorial offenses

In some limited circumstances, Congress has specifically designated the district (within the constitutional limitation) in which venue exists. Some examples of such offenses include the following.

- Flight to avoid prosecution (18 U.S.C. § 1073) (district in which original crime committed or where defendant was detained).
- Capital cases (18 U.S.C. § 3235) (county where the offense was committed, when without "great inconvenience").
- Murder or manslaughter (18 U.S.C. § 3236) (place where injury inflicted).

Venue for territorial offenses where no district is specified by statute is governed by Fed. R. Crim. P. 18. "Unless a statute or these rules permit otherwise, the government must prosecute an offense in a district where the offense was committed." Title 18 U.S.C. § 3237 is a refinement to the general rule, where the offense occurs in more than one district.

> (a) Except as otherwise provided by enactment of Congress, any offense against the United States begun in one district and completed in another, or committed in more than one district, may be inquired of and prosecuted in any district in which such offense was begun, continued, or completed.

Any offense involving the use of the mail, transportation in interstate or foreign commerce, or the importation of a person or an object into the United States, is a continuing offense and, except as otherwise expressly provided by enactment of Congress, may be inquired of and prosecuted in any district from, through, or into which such commerce, mail matter, or imported object or person moves.

In addition, in *United States v Rodriguez-Moreno*, 526 U.S. 275 (1999), the Supreme Court held that the offense of using or carrying a firearm during a predicate crime of violence or a drug trafficking crime can properly be prosecuted in the district where the predicate offense occurred, even though the using or carrying did not occur in that district. This is because the underlying crime of violence is an element of the § 924(c) offense.

With respect to a conspiracy to commit a territorially-based offense, "venue is proper in any district in which an overt act in furtherance of the conspiracy was committed by any of the co-conspirators. . . . The defendant need not have been present in the district, so long as an overt act in furtherance of the conspiracy occurred there." *United States v. Naranjo*, 14 F.3d at 147. *See United States v. Bin Ladin*, 91 F. Supp. 2d 600 (S.D.N.Y. 2000) (venue in Southern District of New York for conspiracy to bomb U.S. Embassies in Africa proper, where overt acts in furtherance of the conspiracy occurred there).

The "continuing offense" principal can include the receipt of phone calls and—the Department believes—e-mail messages in the district where the sender or recipient is located. *See*, *e.g.*, *United States v. Kim*, 246 F.3d 186, 191-93 (2d Cir. 2001) (offense of wire fraud is committed in any district in which transmission is sent or received, even if defendant making the transmissions never enters the country).

Venue determinations are offense specific. Where more than one count is charged in an

indictment, venue must be established with respect to each count. *See United States v. Beech Nut Nutrition Corp.*, 871 F.2d 1181, 1188 (2d Cir. 1989). This principle also governs substantive crimes and conspiracy, even if the substantive offense is in furtherance of the conspiracy. Thus, where *no* element of that offense is committed in the district where the underlying conspiracy occurred, it cannot be joined with the conspiracy for trial. *See United States v. Corona*, 34 F.3d 876, 879-80 (9th Cir. 1994).

D. Venue for extraterritorial offenses

Title 18 U.S.C. § 3238 provides:

> The trial of all offenses begun or committed upon the high seas, or elsewhere out of the jurisdiction of any particular State or district, shall be in the district in which the offender, or any one of two or more joint offenders, is arrested or first brought; but if such offender or offenders are not so arrested or brought in any district, an indictment or information may be filed in the district of the last known residence of the offender or any one of two or more joint offenders, if no such residence is known, the indictment or information may be filed in the District of Columbia.

Several courts have held or suggested that an offense may be extraterritorial under § 3238 when "begun" on the high seas or in a foreign country, even though subsequent overt acts or elements of the offense occur within the United States. *See United States v. Erwin*, 602 F.2d 1183, 1185 (5th Cir. 1979) ("that venue may also be appropriate in another district will not divest venue properly established under § 3238"); *United States v. Bin Ladin*, 91 F. Supp. 2d at 614 n.23 (collecting cases). *But see United States v. Gilboe*, 684 F. 2d 235, 239 (2d Cir. 1982) (dicta). Thus, in circuits that follow this rule, prosecutors may have a measure of latitude in determining whether to allege venue with respect to an offense begun overseas, but involving the commission of subsequent elements in U.S. territory on the basis of § 3237 (pertaining to territorial crimes), or, alternatively, under § 3238 (pertaining to extraterritorial offenses).

E. Options and considerations for determining venue for an extraterritorial offense under § 3238

Indict while the defendant is still overseas. The prosecutor may wish to do so to lock in venue with respect to a particular offense, to stop the running of the statute of limitations, or to satisfy a requirement for extradition. If a defendant is indicted while still abroad, the indictment should ordinarily be returned in the district of the defendant's last known residence (or the last known residence of any indicted codefendant). Where there is no such district (or the former residence cannot be ascertained), venue lies in the District of Columbia.

Use the "first brought" or "arrested" option. It may be advisable to determine the federal district into which the defendant will likely be "first brought" or "arrested," indict in that district, and return him there. In *United States v. Feng*, 277 F.3d 1151, 1155 (9th Cir. 2002), the court held that, regardless of whether an indictment was returned in a particular district before, during, or after the defendant was "first brought" there, venue was proper under the "first brought or arrested" clause of § 3238. The downside to this option is that, in cases where the defendant is actually first brought or arrested in a district other than that where the anticipatory indictment is returned, the indictment is a nullity and the district where the defendant's arrival or arrest occurs governs the venue determination.

Apprehend the defendant and return him to the United States without first indicting him. In such cases, venue lies in the district where the defendant first enters the United States. Bear in mind that the phrase "first brought" means that the defendant *must be returned in a custodial status*. *See United States v. Liang*, 224 F.3d 1057, 1060 (9th Cir. 2000).

Under the "first brought" option, venue is triggered by any incidental stop in the United States, regardless of whether it is the intended destination of the flight returning the defendant from overseas. *See Chandler v. United States*, 171 F.2d 921, 933 (1st Cir. 1948) (brief layover triggers "first brought" venue). Thus, an en route refueling stop can effectively thwart a plan to return the defendant to a particular district for indictment and trial.

The venue by "arrest" option under § 3238 is offense specific. The term "arrested" applies to the

district in which the defendant is first restrained in connection with the offense charged. Thus, if a defendant's case has been venued in a particular district, and the defendant is present in that district awaiting trial, he may be "arrested" there for an extraterritorial offense, with the result that venue for that offense will be in the same district as that for the previously charged crime. *See United States v. Wharton*, 320 F.3d 526, 536-37 (5th Cir. 2003); *United States v. Catino*, 735 F.2d 718, 724 (2d Cir. 1984).

F. Venue analysis

- Is the offense territorial or extraterritorial? If the former, in which district did the offense occur or did it occur in several districts?
- If territorial, is there an option as to the district in which to bring the charges? If so, is one preferable to the others?
- If extraterritorial, does the prosecutor want or need, for some reason, to indict prior to defendant's return?
- If the prosecutor wishes to file a prereturn indictment, which is the appropriate district?
- Are there reasons for wanting to effect the defendant's return to a particular district? If so, does the government want to indict him in that district in anticipation of his being "first brought" in that district?

G. Venue for criminal complaints

A criminal complaint to obtain the extradition of a defendant may be needed. Federal Rules of Criminal Procedure 3 and 4 do not particularize the district in which a complaint can be sought and an arrest warrant obtained for an extraterritorial offense, when an indictment is not first returned. It is advisable to seek process in the district where an indictment is likely to be brought, but it is the Department's position that any U.S. magistrate judge can issue a warrant for an extraterritorial offense, without regard to the location where the indictment is likely to be returned.

IV. International agreements authorizing extraterritorial jurisdiction

A number of international agreements, to which the United States is a party, are designed to thwart acts of terrorism and are enumerated below. The federal legislation that implements those agreements, and the bases under which such legislation authorizes the assertion of jurisdiction over such offenses, are identified. Note that, in a number of instances, federal jurisdiction can vest over a person charged with a treaty-implementing offense merely by virtue of his presence in the United States and without regard to the location of the crime.

- Convention for the Suppression of the Unlawful Seizure of Aircraft ("Hague Convention") (effective Sept. 14, 1971). The "effective dates" connote the dates when the United States became a party to the particular convention. In many instances, the effective date of the implementing legislation is also governed by that date.

  Implementing Legislation—49 U.S.C. § 46502(b) (penalizes commission of any offense embraced by the Hague Convention, such as the seizure or attempted seizure of an aircraft in flight, when outside the "special aircraft jurisdiction").

  Jurisdictional Predicates—commission on an aircraft "in flight," outside of the "special aircraft jurisdiction of the United States," *and* one of the following: (A) a U.S. national was aboard the aircraft; (B) the offender was a U.S. national; or (C) "the offender is afterwards found in the United States." *See Rezaq*, 134 F.3d at 1131-32 (the phrase "afterwards found" includes the defendant's forcible return).

- Convention On Offenses and Certain Other Acts Committed On Board Aircraft, ("Tokyo Convention") (effective Oct. 1, 1969).

  Implementing Legislation—49 U.S.C. §§ 46502(a) (aircraft piracy); 46504 (assault upon or interference with aircrew member); 46505 (carrying a weapon or explosive on an aircraft); 46506 (commission of certain crimes, such as assault, aboard an aircraft).

  Jurisdictional Predicates—49 U.S.C. § 46502 (a)—(A) commission of an offense in the special aircraft jurisdiction of the United States; or (B) attempted commission in the special aircraft jurisdiction although the aircraft is not "in flight" at the time of the attempt, if it would have been "in flight" had the offense been consummated; 49 U.S.C.

§ 46504—commission of the offense "in the special aircraft jurisdiction of the United States;" 49 U.S.C. § 46505—commission or attempted commission of offense on an aircraft in or intended for operation "in air transportation or intrastate air transportation" (The term "air transportation" is defined as "foreign air transportation, interstate transportation, or the transportation of mail by aircraft."); 49 U.S.C. 46506—commission on board an aircraft, in the special aircraft jurisdiction, of an offense punishable if committed in the special maritime and territorial jurisdiction of the U.S. or under the District of Columbia Code.

- Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, ("Montreal Convention") (effective Feb. 23, 1973).

  Implementing Legislation—18 U.S.C. § 32—destruction of aircraft or aircraft facilities.

  Jurisdictional Predicates—§ 32(a)(1) (setting fire to, damaging, destroying aircraft)—any aircraft in special aircraft jurisdiction; or any civil aircraft used in interstate, overseas, or foreign commerce; § 32(a)(2) (placing destructive device on "any such aircraft") *see* subsection (a)(1); § 32(a)(3) (disabling an aircraft navigation facility) must jeopardize "any such aircraft in flight"—*see* subsection (a)(1); § 32(a)(4) (setting fire to, damaging, or placing destructive device on appliances, structures, ramps, etc.)—facility must be used in connection with aircraft defined in subsection (a)(1); § 32(a)(5)(acts of violence against persons on "any such aircraft" if that act is likely to endanger "the safety of such aircraft")—the aircraft must be one defined in subsection (a)(1); § 32(a)(6) (knowing communication of false information that endangers safety of aircraft)—the aircraft must be one defined in subsection (a)(1). Section 32(b) (acts of violence against any individual aboard an aircraft registered in a country other than the United States so as to endanger its safety, destruction of such aircraft, placing destructive device on such aircraft)—jurisdiction where: (1) a U.S. national is on board (or would have been on board the aircraft); (2) the offender is a U.S. national; or (3) "the offender is afterwards found in the United States." *See United States v. Yousef*, 327 F.3d at 88-89 (approving exercise of extraterritorial jurisdiction for placing a bomb on a civil aircraft registered in another county, where defendant was "afterwards found in the United States").

- Protocol for the Suppression of Unlawful Acts of Violence At Airports Serving International Civil Aviation Supplementary to the Convention for the Suppression of Unlawful Acts Against Civil Aviation ("Airport Violence Protocol") (effective Nov. 18, 1994).

  Implementing Legislation—18 U.S.C. § 37—prohibits use of any device, substance, or weapon, to perform an act of violence against a person serving in civil aviation, or damage to airport facilities such that it endangers, or is likely to endanger, safety at that airport.

  Jurisdictional Predicates—(1) the prohibited activity takes place in the United States; (2) the prohibited activity takes place outside the United States and (A) the offender is later found in the United States; or (B) an offender or victim is a U.S. national.

- Convention for the Prevention and Punishment of Crimes Against Internationally Protected Persons (IPP Convention) (effective Jan. 6, 1985).

  Implementing Legislation—18 U.S.C. § 112 (assaults upon or intimidation of foreign official, foreign guest, or internationally protected person (IPP)); 18 U.S.C. § 878 (threats and extortion against a foreign official, official guest, or IPP); 18 U.S.C. § 1116 (murder or manslaughter of foreign official, official guest, or IPP); 18 U.S.C. § 1201(a)(4) (kidnapping of foreign official).

  Jurisdictional Predicates—18 U.S.C. § 112—jurisdiction where victim is a foreign official, "official guest," or IPP outside the United States if: (1) he is an employee or agent of the United States; (2) the offender is a U.S. national; (3) the offender is "afterwards found" in the United States; 18 U.S.C. § 878—as above

(*see* 18 U.S.C. § 878(d)). 18 U.S.C. § 1116—as above (*see* 18 U.S.C. § 1116(c)). 18 U.S.C. § 1201(a)(4)—as above (*see* 18 U.S.C. § 1201 (e)).

- International Convention Against the Taking of Hostages ("Hostage-Taking Convention") (effective Jan. 6, 1985)

  Implementing Legislation—18 U.S.C. § 1203—hostage taking.

  Jurisdictional Predicates—18 U.S.C. § 1203(b).

If the offense is extraterritorial, there is jurisdiction if :(A) the offender or the victim is a U.S. national; (B) "the offender is found in the United States"; (C) the government or organization sought to be compelled is the United States. *See* 18 U.S.C. § 1203(b)(1).

If the offense occurred inside the United States (and there are no other extraterritorial aspects to the offense), there is federal jurisdiction where the entity sought to be compelled is the United States. *See* 18 U.S.C. § 1203(b)(2).

- Convention on the Protection of Nuclear Materials ("Nuclear Materials Convention") (effective Mar. 3, 1980).

  Implementing Legislation—18 U.S.C. § 831—prohibited transactions involving nuclear materials.

  Jurisdictional Predicates—(1) commission of the offense in the United States, the special maritime and territorial jurisdiction, or the special aircraft jurisdiction; (2) the offender or victim is a national of the United States or a U.S. corporation; (3) the defendant is thereafter found in the United States, even if the offense is extraterritorial.

- Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation ("Maritime Safety Convention") (effective Mar. 6, 1995).

  Implementing Legislation—18 U.S.C. § 2280—prohibits, *inter alia*, seizure or exercise of control of a ship by force; acts of violence against a person on board a ship, if likely to endanger the vessel; destruction of the vessel or cargo.

  Jurisdictional Predicates—(1) In the case of a "covered ship" (A "covered ship" is one navigating or scheduled to navigate into, through or from waters beyond the territorial sea of a single country, or a lateral limit of that country's territorial sea with an adjacent country." 18 U.S.C. § 2280(e))—there is jurisdiction if: (A) the activity is committed (i) against or on board a ship flying the U.S. flag; (ii) in the United States; (iii) by a U.S. national or a stateless person who habitually resides in the United States; (B) during the commission of such activity, a U.S. national is seized, threatened, injured, or killed; or (C) the offender is later found in the United States. (2) In the case of a ship navigating or scheduled to navigate solely within the territorial sea or international waters of a country other than the United States, if the offender is later found in the United States after such activity is committed; and (3) in the case of any vessel, if the activity is committed in an attempt to compel the United States to do, or abstain from doing, any act.

- Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf ("Fixed Platform Protocol") (effective Mar. 6, 1995). A "'fixed platform' means an artificial island, installation, or structure, permanently attached to the seabed for the purpose of exploration or exploitation of natural resources or for other economic purposes." 18 U.S.C. § 2281(d), para. 2.

  Implementing Legislation—18 U.S.C. § 2281—prohibits, *inter alia,* efforts to seize control of a fixed platform, commit an act of violence against persons on board a fixed platform, or commit other acts likely to endanger its safety.

  Jurisdictional Predicates—*See* 18 U.S.C. § 2281(b). (A) the fixed platform is located on the continental shelf of the United States; (B) the platform is located on the continental shelf of another country, but the offense is committed by a U.S. national or a stateless person who habitually resides in the United States; (C) the victim of any such activity is a U.S. national; (D) the platform is located outside the U.S. continental shelf, but "the offender is later found in the United States."

- Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction ("Chemical Weapons Convention") (effective Apr. 29, 1997).

  Implementing Legislation—18 U.S.C. § 229 (prohibits development, production, stockpiling, retention, use or threat to use any chemical weapon, with certain exceptions and exemptions).

  Jurisdictional Predicates—(1) the offense takes place within the United States; (2) the offense is committed by a U.S. national outside the United States; (3) the offense is committed against a U.S. national outside the United States; (4) the offense is committed against property outside the United States that is owned, leased, or used, by the United States or any U.S. department or agency.

- Convention on the Marking of Plastic Explosives for the Purpose of Detection ("Plastic Explosives Convention") (effective June 21, 1998).

  Implementing Legislation—18 U.S.C. § 84l (prohibits manufacture of unmarked plastic explosives); 18 U.S.C. § 842(m) (prohibits importation of unmarked plastic explosives); 18 U.S.C. § 842(n) (prohibits transfer or receipt of unmarked plastic explosives); 18 U.S.C. § 842(o) (prohibits possession of unmarked explosives).

  Jurisdictional Predicates—None stated—by virtue of the nature of the offenses, jurisdiction not extraterritorial.

- International Convention for the Suppression of Terrorist Bombings ("Terrorist Bombing Convention") (effective June 26, 2002).

  Implementing Legislation—18 U.S.C. § 2332f (prohibits placing or discharging an explosive in a public place with the intent to cause death or serious bodily harm or extensive destruction, and such destruction results, or is likely to result).

  Jurisdictional Predicates—*See* 18 U.S.C. § 2332f(b). (1) The offense occurs in the United States and (A) it is committed against another state or facility of such state; or (B) is committed in an attempt to compel another state or the United States to do, or abstain from doing, an act; (C) the offense is committed on board a vessel flying the flag of another state, an aircraft registered in another state, or belonging to another state; (D) the perpetrator is found outside the U.S.; (E) the perpetrator is a national of another state or a stateless person. (2) The offense occurs outside the U.S. and (A) the perpetrator is a U.S. national or stateless person habitually residing in the United States; (B) a victim is a U.S. national; (C) the perpetrator is found in the United States; (D) the offense is committed in an attempt to compel the United States to do, or to abstain from doing, an act; (E) the offense is committed against a state or government facility of the United States; (F) the offense is committed against a U.S. flag vessel or U.S. registered aircraft; (G) the offense is committed on board a U.S. operated aircraft.

- International Convention for the Suppression of the Financing of Terrorism ("Terrorist Financing Convention") (effective June 25, 2002)

  Implementing Legislation—18 U.S.C. § 2339C (prohibits providing or collecting funds with the intention or knowledge that such funds are: (A) to be used to carry out an act which constitutes an offense under one of a number of enumerated treaties relating to terrorist activity; or (B) any other act intended to cause death or serious bodily injury to any civilian or any other person not taking part in hostilities, when the purpose of the act is to intimidate a population, or to compel a government or international organization to do, or abstain from doing, an act).

  Jurisdictional Predicates—*See* 18 U.S.C. § 2339C(b). There is jurisdiction over such offenses when: (1) the offense takes place in the United States and (A) the perpetrator was a national of another nation or a stateless person; (B) on board a vessel flying a foreign flag or an aircraft registered under the laws of another state; (C) on board an aircraft operated by another state; (D) the perpetrator is found outside the United States; (E) was directed toward or resulted in the carrying out of a predicate act against: (i) a national of another state; (ii) another state or government facility; (F) was directed

toward or resulted in the carrying out of a predicate act committed in attempt to compel another state or international organization to do, or abstain from doing, any act; (G) was directed toward or resulted in the carrying out of the predicate act: (i) outside the U.S.; or (ii) within the U.S., and either the offense or the predicate act was conducted in, or the results thereof affected, interstate or foreign commerce; (2) the offense takes place outside the United States and (A) the perpetrator is a U.S. national or a stateless person who habitually resides in the United States; (B) a perpetrator was found in the United States; or (C) was directed toward or resulted in the carrying out of a predicate act against (i) U.S. owned, leased, or used property; (ii) any person or property within the United States; (iii) any U.S. national or the property of such national; (iv) any property of a legal entity organized under U.S. law, including any state; (3) the offense is committed aboard a U.S. flag vessel or a U.S. registered aircraft; (4) the offense is committed on board an aircraft operated by the United States.; (5) the offense was directed toward or resulted in the carrying out of a predicate act committed in an attempt to compel the United States to do, or abstain from doing, any act.❖

ABOUT THE AUTHOR

❑**John De Pue** joined the Criminal Division's Appellate Section in 1978. Eleven years later, he joined the Criminal Division's General Litigation Section as its senior legal advisor for counterterrorism and, upon the establishment of a Counterterrorism Section in that Division, served as its principal appellate advocate. In that capacity, he litigated several of the Department's major cases involving the assertion of extraterritorial jurisdiction. Prior to joining the Department of Justice he served in the Army's Judge Advocate General Corp in the Republic of Viet Nam and taught international law at West Point. He retired from the Army Reserve in 2000 with the rank of Brigadier General, and from the Department of Justice in 2005. He subsequently returned to duty with the Justice Department as an annuitant.✠

Counterterrorism Cooperation Between Allies: A Game Theory Illustration

Jeff Breinholt
Deputy Chief
Counterterrorism Section
National Security Division

I. Introduction

The various commissions that studied the government failings that contributed to the World Trade Center and Pentagon attacks found fault with how intelligence was handled within the U.S. intelligence community. These studies led to structural changes designed to assure that information flows more freely to personnel capable of connecting the dots, in hopes that better information will result in more effective counterterrorism operations. Except in passing, the commission studies have generally not delved in to the structural features of the intelligence and law enforcement communities, the incentives that developed among the players within these structures to hoard or share

information, and the extent to which these factors or structures drive this behavior. Instead, too many panel reports make the mistake of placing a more complex environment into a binary system. Those who, before 9/11, refused to share information were wrong. Those who pushed for greater dissemination were prescient. This assessment is as simplistic, since it overlooks legitimate reasons why information-sharing limitations arise.

This article considers this issue in the context of bilateral counterterrorism cooperation, and the issue of information-sharing between allied nations. I seek to go beyond the binary classification to consider how information-sharing barriers might be redressed through economic analysis. As I will show, it is not enough for two countries to insist that they are fully cooperative with each other in important law enforcement issues. Even very close allies have legitimate reasons for refusing to sharing terrorism-related information. The challenge is to understand these reasons and to evaluate whether the underlying concerns can be accommodated in a way to make bilateral cooperation possible. This is where economic theory can be useful.

For federal prosecutors, there are really two separate concepts—international cooperation against terrorism and information-sharing—that must be understood in order to assess the dynamic that comes into play, and deal effectively with foreign counterparts. One way of understanding this dynamic is an application of game theory, a tool that over the last few decades has been applied to legal analysis. Martin Shubick, *Game Theory, Law, and the Concept of Competition*" U. CIN. L. REV. (Fall 1991). Game theory is the study of the basic elements of conscious conflict and cooperation among multiple people. It seeks to answer complicated questions through the lens of a simple competition, and the strategy that comes into play by rational actors. Game theory analysis results in the establishment of an "equilibrium," which is the strategy that would, and should, be adopted by the players, based on their rational assessment of costs and benefits of the various choices available to them in the game. Where the equilibrium is not the most mutually beneficial, the game theorist seeks to explain what circumstances led to this result. This analysis can lead to the discovery of institutional reforms. For American terrorism prosecutors, game theory offers insight into the type of interactions with foreign counterparts that we might push to institutionalize.

What does game theory suggest about the ideal set of circumstances for fighting terrorism through international cooperation? As shown below, the factors that influence how terrorism-related intelligence flows between two countries are complex, and bilateral counterterrorism cooperation is not subject to binary choices, as may appear at first glance. Game theory analysis suggests some institutional reforms and concepts that will maximize the prospect of an optimal equilibrium. One such concept is what we refer to as the "silver bullet" concession: a commitment by the recipient country that the source country will maintain control over the use of the intelligence it is sharing, including the right to pull it when it appears that an unpalatable amount of disclosure is being threatened in the course of the other country's domestic legal proceedings. It is my hope that we start to institutionalize the silver-bullet concession in case-related international legal assistance.

II. The assumptions: two allied countries, each with an intelligence service

Game theory illustrations require a series of assumptions.

The first assumption in the counterterrorism cooperation scenario is that the players are two allied countries that are jointly interested in fighting international terrorism. Because they are allies and have a mutual goal (and common enemy), each is motivated to help the other, as long as it can be done in a way that is consistent with their own national security.

Each country has an intelligence capability, which means that it invests resources in the collection and analysis of information used to protect its citizens and assets from threats. Although intelligence is sometimes shared with other nations, such sharing is generally done in a manner designed to prevent the recipient country from becoming aware of the sender's specific intelligence-collection capability. In fact, so sensitive is some of the intelligence that it is not shared within anyone outside the country. Within the United States, for example, certain classified documents are marked with the letters "NOFORN," an abbreviation for "No Foreign Dissemination." This subclassification denotes that the document contains information that should not be shared with foreign partners. This decision is based on the fact that the particular

sources and methods of its acquisition will be jeopardized by such sharing, even between allied countries. In intelligence parlance, there is a concept known as "singular intelligence." Information is considered "singular" if its mere dissemination will allow the recipients to know how it was collected. Thus, singular information is more sensitive, and less disseminated, than nonsingular information.

Each country owns all of the intelligence it collects. It has an interest in maintaining its sources and methods as long as possible, because it expends resources developing them. As a result, it is impossible for one country to legally compel intelligence collected by another. Such sharing is only accomplished by consent. Consent, of course, can be obtained by diplomatic, military, or economic pressure.

The fact that the two countries are allies, and equally committed in the battle against international terrorism, does not mean that they share intelligence with each other, as each country's intelligence capability represents an extension of its sovereignty. Thus, each side takes precautions against its intelligence being stolen by other countries, including its closest allies. For example, if a nation catches a spy attempting to steal intelligence on behalf of a friendly foreign country, the spy will be prosecuted. This is necessary, because the disclosure of certain purloined information—even to a trusted ally—ruins certain sources and methods forever. This point is illustrated by the American prosecution of Jonathan Pollard, a former National Security Agency analyst convicted of spying for Israel. *See U.S. v. Pollard*, 959 F.2d 1011 (D.C. Cir. 1992).

The effectiveness of each country's intelligence community is judged by how often it provides intelligence that is useful to operational decision-makers. Each country has adopted an intelligence system that rewards relevant personnel for obtaining information and analysis that proves useful in taking proactive government action. That is, the intelligence collectors and analysts within each country are trained in such a way that they yearn to have their products used for the larger good. Meanwhile, each country also has operational decision-makers who appreciate intelligence—judged by volume, source reliability and track record, and internal consistency, among other factors—that can be used to justify a particular action. This means that, when people who occupy comparable positions in each country's intelligence apparatus get together, they speak the same professional language. They can immediately grasp the relevance of intelligence that is discussed, based on their training.

Note that the above description illustrates the limitations of the binary choice described by President Bush. With these assumptions, which approximate reality, the fact that a country is a close ally of the United States—in the President's words, "with us"—does not mean that every request for terrorism-related intelligence will necessarily be honored.

III. Stag Hunt

Within game theory, there is a useful paradigm, called Stag Hunt, to illustrate the dynamic of intelligence-sharing between countries, under the foregoing assumptions.

It works like this: two people are hunting at the same location. Before the hunt starts, they are not in communication with each other. Each must decide unilaterally whether to be outfitted to hunt a *stag* (a larger game animal) or a *hare* (a rabbit). Successfully hunting a stag requires the cooperation of another person, who must be outfitted accordingly. A single player can successfully get a hare alone, with the proper hare-hunting equipment. A hare, however, cannot be killed with stag-hunting equipment. For the two players, the payoff of a single stag (meat worth $4 each) is greater than what they would receive if they each caught their own hare (meat worth $2 each). Each player, then, is faced with a binary choice, without the benefit of knowing what the other chooses. The matrix showing the contingencies and payoffs is depicted like this:

	Player 2 Choice: Stag	**Player 2 Choice: Hare**
Player 1 Choice: Stag	Player 1: $ 4 Player 2: $ 4	Player 1: $ 0 Player 2: $ 2
Player 1 Choice: Hare	Player 1: $ 2 Player 2: $ 0	Player 1: $ 2 Player 2: $ 2

The best result would be for both players to cooperate, and choose to rent the stag-hunting equipment. Killing a stag would yield $8 worth of meat, $4 per person. However, they cannot

communicate in order to confirm the other's cooperative attitude. What if one opts for the stag-hunting equipment, only to find that the other player is loaded for hare? That person would be out of luck, and would suffer a day without any payout. If a person is sufficiently risk averse or cynical about human nature, he or she might conclude that the other player is going to practice pure self-interest. If this is the case, the best option would be to hunt for hare, where the payout does not depend on any cooperation, although it will be lower.

The Stag Hunt game is intentionally unreal, as there are very few situations in which communication necessary for cooperation is impossible. However, it illustrates the dynamic that is at play in the question of intelligence-sharing among countries that are jointly interested in combating international terrorism. A completely self-interested strategy means no cooperation.

Assume that two countries with an intelligence apparatus and a mutual goal of fighting terrorism must decide whether to share sensitive intelligence, and that the decision must be made in the context of the Stag Hunt game. If both countries agree to cooperate, the pooling of intelligence may allow them to connect the various pieces of a developing terrorist plot so that law enforcement from one of the countries may prevent it. If one country refuses to cooperate, both countries may suffer a loss of sources and methods, without either receiving the benefit of a full pooling of information.

IV. Application of the game: building a structure for optimal equilibrium

The Stag Hunt illustrates a situation where no communication is permitted between the players. Moreover, each game ignores the iterative nature of communication, where players make a series of moves that are informed by the other player's choices. In the real world, this is represented by the give and take of negotiation. In game theory, this is referred to as the "extensive form" game model. In this model, players have an opportunity to assess and recalibrate their strategy over the course of repeated interactions.

Let's return to the set of assumptions described for the international counterterrorism cooperation example, and add a few more. The two countries are contiguous, citizens from one country often travel to the other, and the two countries often play host to the same visitors. As a result, the intelligence each country collects domestically is likely to have operational significance to the other. Assume further that, due to the actions of one country, its neighbor realizes that it has intelligence which, if shared, will create some counterterrorism options that would not otherwise exist.

A discussion of hypothetical countries that qualify for the series of assumptions we have posited follows. The country of South has announced the indictment of a group of individuals involved in a credit card fraud scheme, and this news is widely publicized. What is not publicized is the fact that South has additional intelligence on these defendants, developed though its sensitive sources and methods. Although South's intelligence suggests that the credit card scheme is part of a terrorist financing operation, there is not enough intelligence yet to justify seeking charges on South's crime of "providing material support." *See* 18 U.S.C. §§ 2339A, 2339B. For this, South needs additional evidence.

News of the credit card fraud prosecution reaches North's intelligence service personnel, who realize that they have information suggesting that some of the South defendants are receiving directions from a North-based Al Qaida operative, who, in turn, is speaking by phone to Al Qaida leadership in Afghanistan. This is something that South suspects, based on the fragmentary information collected through its personnel. One of North's most guarded national security secrets is how the North intelligence service obtained this information. As a result, it does not part with this information lightly. North's intelligence service personnel telephone South's intelligence service and say that is has classified intelligence related to the individuals recently charged with credit card fraud. No further elaboration is given.

Unlike the Stag Hunt, the reality is that these two countries can communicate, at least up to a point. This means that the scenario will take the extensive form.

Advised of the news from North, the first exchange starts with a phone call from South.

_____

South: We want your intelligence, to share with our prosecutors.

North: No.

_____

If the dialogue ended at that point, there would be an equilibrium with no payout on either side. South does not obtain the benefit of the North's intelligence. Each country breaks even (except for the *de minimis* cost of a long-distance phone call). Nothing ventured, nothing lost.

This equilibrium, however, is not ideal. What if North's information about South's defendants, when combined with the more fragmentary South intelligence, could have been used to thwart a terrorist plot? What if the plot results in a sensational attack, with hundreds of innocent civilians dead in both South and North? Personnel involved in the decision not to share intelligence that could have disrupted the attack will have quite a bit of explaining to do. They will likely become professional witnesses before various commissions and legislative bodies in both countries.

When the initial request is rejected, South's diplomats enter into negotiation. Perhaps the diplomats repeat the South's President's statement that you are either for or against us, in hopes that North's intelligence officials will reconsider their rejection. Assume (again, unrealistically) that South's negotiators are not authorized to give assurance as to how South's prosecutors will use North's intelligence, if they are fortunate enough to receive it. This means that North's reaction is limited to a binary choice, a yes or no answer, and that North has no way to control how South will use North's intelligence once it is disseminated. If this occurs, South will be faced with a unilateral choice: either use the intelligence to supersede the criminal charges, or do not use it. Assume that South's decision will not be informed by the preferences of North's intelligence.

With two players each facing a binary choice, there are four possible scenarios arising from this point.

- Scenario 1: North persists in saying no.
- Scenario 2: The intelligence is shared. South uses it in criminal prosecution.
- Scenario 3: The intelligence shared. South does not use it.

Placed within the Stag Hunt analysis, these scenarios translate into this 2 x 2 matrix.

	North: Share Intelligence	North: Do not Share
South: Use It	Scenario 2	Scenario 1
South: Do not Use It	Scenario 3	Scenario 1

In Scenario 1, there is no payout or costs for either player (other than the costs which would be assessed if the failure to share information is later determined to be part of a failure to prevent a terrorist attack). Scenario 1 is, however, probably the worst situation. South and North are two allied, contiguous nations committed to fighting international terrorism, yet they cannot reach an agreement to share information that is of joint interest. To avoid this embarrassment, the countries have incentive to try to negotiate conditions to avoid Scenario 1.

Consider Scenario 2, where South makes the unilateral decision to use the information. What are the respective costs and benefits to each side? North's government has assisted in a South terrorism case, which benefits North. North's intelligence service has found a worthy consumer for its products, which is another benefit. The cost to North for this decision, however, is likely the permanent loss of the sources and methods that gave rise to this intelligence, because South's decision to use it is made without regard to North's intelligence concerns or equities.

Whether Scenario 2 is a good situation for North will depend on whether the benefits exceed the costs. Because North was not involved in the decision of how and if South's prosecutors would use the information in judicial proceedings, it had no way to measure the bottom-line impact of Scenario 2. On the other hand, Scenario 2 gives South the payout of intelligence to use in a criminal prosecution. There is not much cost, if one does not count the damage to the future willingness of North to provide this type of intelligence, in light of the resulting damage to its sources and methods.

In Scenario 3, North's intelligence is shared, but not used by South. This means that the cost to North is small, since the sharing of the intelligence did not result in its publication, and any loss of sources and methods would be limited

to that portion which it would otherwise have treated as NOFORN (unclear from these facts). What about the benefits to North? There are none, other than the goodwill it engendered with South. What is also unclear is what went into South's decision not to use the intelligence. It may have arisen from the fact that there was no mechanism for obtaining North's assistance to place the intelligence into an admissible form for South's judicial proceedings. For example, North's intelligence may have been shared in raw form, making it hearsay and difficult to properly authenticate under South's evidentiary rules. Of course, North's intelligence service could provide a witness, a prospect that might involve cross-examination of the witness and the risk of an unpalatable amount of disclosure of national security secrets. Although there might not be a cost for South, there would undoubtedly be frustration at possessing intelligence it could not use, because there was no mechanism for obtaining additional assistance from North.

The discussion of Scenarios 2 and 3 suggests a third round of play in which the countries negotiate further conditions that will justify their decision to cooperate. Given the foregoing assumptions and facts, and the unknown factors that prevent a full analysis of Scenarios 2 and 3, the conditions should permit North to maintain a certain amount of control over how South's prosecutors use the North's intelligence, and allow South's prosecutors to obtain additional assistance from North so that the intelligence can be effectively exploited in a judicial proceeding.

The negotiation would look like this.

———————

South: *We want your intelligence, to share with our prosecutors.*

North: *No.*

South: *Our President says that, in the fight against international terrorism, you are either with us or against us. Each of our nations face a common enemy, and this is an important opportunity. If we fail to cooperate and terrorists strike, the media and historians on both sides of the border will be dancing on our graves.*

North: *O.K. How about this? You can see this information, but your prosecutors cannot use it unless you convince us that it will be done in such a way that our national security interests—the sanctity of our sources and methods—will be maintained.*

South: *How can we do that?*

North: *We will let you examine the intelligence, but your use of it will be contingent on our ability to prevent you from using it, if and when it becomes clear that such use will involve an unpalatable amount of disclosure in any resulting judicial proceedings, of our intelligence collection capabilities.*

South: *Alternatively, you give us the information and our prosecutors will review it. If they decide that it justifies the addition of terrorism charges to our indictment, they will explain to you how they plan to present it in court. They will walk your lawyers through their specific plans and strategy. They will also try to minimize the uncertainty in what the court will require to authenticate and admit that information, by seeking an advance court ruling on its admissibility. By the time of the trial, we will all know what is required.*

North: *What if these plans break down when it comes to the trial? What happens if a witness we provide to help you introduce this intelligence is subject to cross-examination? How will we protect against the prospect that our witness may be forced by the judge to testify about our state secrets?*

South: *How about this? Even after the start of the trial, you will maintain an unfettered right to prevent us from introducing your intelligence, including the right to force us to pull that information from the criminal proceeding if it appears, in your judgment, that our court is*

permitting an unpalatable amount of disclosure. We will honor our commitment to you, even if our prosecutors have to suffer the most extreme judicial sanction—the dismissal of the prosecution. This way, we get to review and possibly use the intelligence you have collected, you maintain the right to control that intelligence consistent with your national security interests, and we each gain the joint benefit of fighting terrorism through bilateral cooperation.

North: I think we have a deal.

———————

This is the equilibrium that is reached through negotiation, something that is not permitted by the classic Stag Hunt model. By changing the dynamic to allow for communication in the context of the sharing of counterterrorism intelligence between two allied countries, and considering the rational moves by each, we have used game theory to construct the optimal infrastructure to reach the most mutually beneficial equilibrium.

The optimum is reached by the requesting country's (South) willingness to concede to the providing country (North) the unfettered right to maintain control over the requesting country's use of the intelligence in any resulting legal proceeding, as a condition of it being permitted to review it in the first instance.

This is close to an existing intelligence concept known as "originator-controlled" information (ORCON). Intelligence labeled in this way cannot be used or disseminated without the consent of the originator. The optimal equilibrium will be reach in this situation if South is willing to grant ORCON assurances to North, as a condition of examining its intelligence.

If South grants ORCON assurances, Scenario 1 is avoided entirely. The intelligence is shared.

From there, whether the ultimate resolution will be Scenario 2 or Scenario 3 is not known, since this depends on factors that are beyond the control of the parties at the time of the agreement. ORCON assures that Scenario 3 will be reached, however, only if it is more mutually beneficial than Scenario 2. Getting to Scenario 3 requires a willingness of North to give permission for South to use the information in the judicial proceeding, which is based on North's assessment of the costs (where any uncertainty has been minimized by pretrial litigation). What little risk remains is offset by the ability of North to make the unilateral decision to withdraw consent of the use of the intelligence. This means that it can exercise its ORCON rights at its own discretion. If Scenario 3 is reached—the best one for South—it will also necessarily be the best one for North. The negotiations assure this result.

It is a beautiful thing. A set of rationally-negotiated conditions has been set in which everyone wins, except the terrorists.

V. Reality: The Charlotte Hizballah Case

Shortly before the turn of the Millennium, when the United States was on a heightened state of alert, an American customs official in Washington state noticed something strange about a foreign traveler seeking to enter the United States on an automobile ferry at the northwest border. The traveler's attempt to physically escape the officer's questioning was unsuccessful, and the officer uncovered explosive materials in the trunk of the traveler's car. Ahmed Ressam, an Algerian who had spent time in Canada, was ultimately convicted of an Al Qaida plot to blow up Los Angeles International Airport. The result was aided by assistance from the Canadian government. *See U.S. v. Ressam*, 221 F.Supp.2d 1252 (W.D.Wash. 2002).

Although the Ressam case received more attention, there was another case on the east coast of the country that was perhaps even more significant, at least in terms of the long-term implications for international cooperation. It involved a group of Hizballah operatives in North Carolina. The group was led by Mohamad Youssef Hammoud, and came to the attention of the authorities because of an interstate cigarette smuggling operation uncovered by an off-duty sheriff.

Hammoud and his associates bought large quantities of cigarettes in North Carolina, smuggled them to Michigan, and sold them without paying Michigan taxes. They took advantage of the fact that Michigan imposes a tax of $7.50 per carton of cigarettes, while the North Carolina tax was only 50 cents. Before their arrest on federal racketeering charges, the plotters transported cigarettes valued at roughly $7.5 million, depriving the state of Michigan of $3 million in tax revenues. During this period,

Hammoud led weekly prayer services for Shi'a Muslims in Charlotte at his home, where he would urge the attendees to donate money to Hizballah. Hammoud would then forward some of the money to Hizballah leaders in Beirut. In addition to the RICO charges, Hammoud was ultimately charged with various immigration violations, sale of contraband cigarettes, money laundering, mail fraud, credit card fraud, and conspiracy to provide material support to Hizballah. *See United States v. Hammoud*, 381 F.3d 316, 326-27 (4th Cir. 2004). It became the first American terrorist financing case to ever go to trial.

At the trial, the prosecutors called a childhood friend of Hammoud, Said Harb, to describe the cigarette smuggling operation and Harb's efforts to assist Hizballah in obtaining "dual use" equipment, such as global positioning systems, which could be used for both civilian and military activities. Harb testified that Hammoud declined to become involved in providing equipment—which occurred in Canada—because he was helping Hizballah in his own way. However, when Harb traveled to Lebanon in September 1999, Hammoud gave him $3,500 for Hizballah. *Id*. at 327. The prosecutors also introduced summaries and analyses of conversations captured electronically through surveillance conducted by the Canadian Security Intelligence Service (CSIS). A number of these CSIS recordings were destroyed pursuant to routine procedures. Fortunately, summaries and analysis of the conversations were prepared by a CSIS communications analyst shortly after each conversation was recorded. During pretrial proceedings, the district court ruled that the CSIS summaries were admissible as recorded recollections, Fed. R. Evid. 803(5), and as public records. *See id.* Rule 803(8).

At Hammoud's trial, the prosecutors introduced the factual portions of some of these summaries (the analysis was redacted from the summaries before submission to the jury). Hammoud stipulated to the admissibility of the summaries. 381 F.3d at 335. The CSIS wiretaps showed a procurement operation involving Harb was overseen by Hizballah's Chief of Procurement from Lebanon, Hassan Laqis, and carried out by an operative trained by Iran's Revolutionary Guard, Mohamad Dbouk. The CSIS information showed that Hizballah wired tens of thousands of dollars from Lebanon to Canada for the purchase of the dual-use equipment. Later in the procurement efforts, Hizballah entered into an agreement with its operatives in Canada to purchase equipment with fraudulent credit cards, and pay fifty cents on the dollar for all items procured. *See* D. Scott Broyles and Martha Rubio, *Smokescreen for Terrorism*, 52 UNITED STATES ATTORNEYS' BULLETIN 30 (Jan. 2004).

Thus, *Hammoud* directly involved the dynamic discussed above. Canadian intelligence, specifically electronic surveillance, offered American counterterrorism officials insight into the operations of a U.S.-based Hizballah cell. This intelligence was so good that the Americans used it in the criminal prosecution of the cell leader. What went into that decision?

The public answer to that question comes from a book by Tom Diaz and Barbara Newman. TOM DIAZ & BARBARA NEWMAN, LIGHTNING OUT OF LEBANON: HEZBOLLAH TERRORIST ON AMERICAN SOIL (2005). The U.S.-Canadian negotiations essentially mimicked the negotiations between North and South, after the ban on communication in the Stag Hunt game was lifted.

CSIS used wiretaps and other communications intercepts to monitor the activities of Hizballah operatives within Canada. In 1999, it learned that the Hizballah dual-use procurement involved Said Harb, an American who had traveled to Vancouver from Charlotte. It notified the FBI, which quickly realized the significance of the intelligence. The FBI knew that Harb was tied to Hammoud, who was charged with racketeering, but not yet terrorist financing. The American prosecutors believed that Harb would be a valuable prosecution witness if he could be convinced to cooperate against Hammoud, and that the CSIS electronic intercepts—never before used in any American or Canadian judicial proceeding—could be useful in convincing Harb that he had no choice but to cooperate.

As Diaz and Newman describe it, "An intricate dance thus commenced in the spring of 1999. A rolling American team of FBI investigators and Justice Department lawyers shuttled to Canada to court the Canadians. By the summer of 2000, the dance turned into a race against time." *Id.* at 207.

The assurances that ultimately led to the deal was referred to as the "silver bullet." In exchange for granting American prosecutors the right to use the Canadian intelligence, CSIS lawyers were assured that they could withdraw the Canadian intelligence from the case at the first suggestion

that the presentation of the evidence would imperil Canada's security. *Id.* at 216. The U.S. prosecutors promised to seek a pretrial ruling from the court in North Carolina on precisely what information needed to be presented in order to successfully admit the Canadian intelligence as one of the hearsay exceptions under the Federal Rules of Evidence. This was accomplished prior to Harb's February 2001 guilty plea. A year later, Harb testified against Hammoud, who was ultimately convicted. Harb received a three and one-half year sentence. Hammoud ultimately received a sentence of over 150 years, which he is currently appealing. *Id* at 217.

VI. Institutionalizing the "silver bullet"

It is sometimes said that great cases make bad law. This is certainly not true of the Charlotte Hizballah case, which represents an anecdotal example of two allied countries coming together in an effort to fight a common threat, and creative thinking about how intelligence can be transformed into evidence admissible in a criminal trial. What does it say about bilateral counterterrorism cooperation generally? Can these lessons from Charlotte be institutionalized?

In *Hammoud*, the solution was the "silver bullet." CSIS lawyers maintained an unfettered right to pull back Canadian intelligence if it appeared, during the American judicial proceedings, that Canadian national security was about to be compromised. Recall, in the hypothetical dialogue between North and South, this was the last promise made by the country seeking permission to use the intelligence, a concession that ultimately clinched the deal.

The "silver bullet" is essentially the reaffirmation of "originator controlled" (ORCON) limits on dissemination. Under ORCON, the originator of intelligence does not lose control over how it is used merely by disseminating it. Instead, the receiving entity agrees, as a condition of gaining access to the intelligence, to be bound by the originator's conditions on use, and to not disseminate it to any third-party absent the originator's permission. As shown in Part III, once we lift the ban on players' communication that prevents a certain optimization in the Stag Hunt model and play the game forward, the negotiation of ORCON conditions will result in the most beneficial equilibrium.

To illustrate, consider the cost/benefits to each side of the negotiations. The cost of dissemination subject to ORCON is close to zero for the originator, since it maintains control over whether and how the intelligence is used by the receiving party. The originator gives up nothing. This means that any positive benefit will make that choice worthwhile. There will always be some benefit to sharing intelligence, since it means that the originator has found a consumer, one of the assumed goals of its intelligence apparatus. The size of the benefit will vary, from small (the recipient country is ultimately unable to use it) to large (the intelligence is used to obtain a significant counterterrorism result). In general, with ORCON assurances, the benefit to the originator will exceed the cost, which makes a decision by the originator to share the information easy.

Consider the cost/benefit for the requesting party from the following two scenarios.

- The requesting party refuses to grant ORCON assurances.
- The requesting party agrees to grant ORCON assurances.

In the first situation, if it is agreed that the originator's decision to share the intelligence will depend on ORCON assurances, the intelligence will not be forthcoming. In the second, the requesting party receives the intelligence, but it is subject to originator controls.

Receiving the intelligence, even if its value is limited by ORCON controls, is better than not receiving it, since there is the benefit of having pertinent knowledge. What about the cost? The cost of granting ORCON assurances is whatever will be incurred in seeking the originator's permission prior to using the information, as opposed to maintaining the unilateral right to decide whether to use the intelligence that is shared. The cost, however, will always be exceeded by the benefit, because the cost is a necessary condition to receiving the information, without which there will be no benefit. Also, if the costs of obtaining additional permission from the originator do not exceed the benefit of using the information, the intelligence can be shelved. If the requesting party refuses to grant ORCON assurances to the originator, it will remain ignorant of the intelligence, and will be deprived of engaging in a later cost/benefit analysis.

This analysis illustrates the benefits of the institutionalization of ORCON assurances, a practice that may not seem intuitive in the

absence of game theory analysis. Countries should be generous is giving ORCON assurances to their allies if it increases the sharing of intelligence. In *Hammoud*, the "silver bullet" assurances came from U.S. prosecutors. Should lawyers be authorized to bind the entire U.S. Government in their negotiations with other countries' intelligence services? Binding the U.S. Government to certain legal positions is what federal prosecutors do everyday, in making decisions to grant immunity or enter into plea agreements. Why should they not be permitted to grant ORCON assurances to foreign intelligence services?

The implication of this analysis is that greater and more meaningful counterterrorism cooperation between allied nations is possible through a decision to institutionalize ORCON controls, and a mutual understanding of each countries' discovery obligations and evidentiary rules that make operations decisions a truly collaborative process.

VII. Conclusion

Game theory tools and the Stag Hunt scenarios show the cost of uncertainty. In these cases, uncertainty results from the rules of the games, where the players are unable to communicate. These rules can lead to player decisions that mimic what would occur in a "zero-sum game." A zero-sum game is one in which a gain for one participant is always at the expense of another, such as in most sporting events. In such a situation, the equilibrium cannot satisfy both players. When it is applied to the concept of international cooperation by allied nations against terrorism, it illustrates the dangers the United States simply cannot afford. In a zero-sum game, allies are transformed into adversaries. If each has a piece of a larger puzzle, the adversarial relationship will result in a failure to connect the dots or solve the puzzle.

Fortunately, game theory illustrates a way out of this darkness. Bilateral counterterrorism cooperation need not be a zero-sum game, at least if it involves countries with a history of trusting each other. In this situation, they are able to communicate and agree to a set of conditions that will eliminate uncertainty. Where this is possible, the equilibrium will be the result of negotiation, with each side being rationally self-interested and aware of the other's moves.

The negotiation depicted in this article shows the fallacy of viewing international counterterrorism cooperation and information-sharing as a binary choice. Effective cooperation requires recognition of the iterative nature of bilateral cooperation, and the very real risks that arise when countries decide to share their intelligence sources and methods. Managing this risk requires conditions to assure that each side is able to maintain its equities in the face of the actions of the other.

The hypothetical negotiations suggest an ideal equilibrium. Intelligence is shared, but it remains subject to control by the originator, which maintains a role in the recipient's decision-making process concerning the use of the intelligence. This ideal has an added benefit: the recipient country is not left alone when facing the mechanical challenge of using the information. For example, if the intelligence may be potentially useful as evidence in a judicial proceeding, the ORCON assurances imply a mechanism for the originator's involvement in the solution—locating and negotiating with the proper foundational witness, a burden that will not be borne solely by the recipient. In the end, each side maintains its right to protect its sovereign equities while maximizing the opportunity for effective joint counterterrorism operations.❖

ABOUT THE AUTHOR

❑**Jeff Breinholt** is Deputy Chief, Counterterrorism Section, National Security Division, and heads the Terrorist Financing Unit. He joined the Department of Justice with the Tax Division, Western Criminal Enforcement Section in 1990 and spent six years as a Special Assistant U.S. Attorney for the District of Utah before joining the Counterterrorism Section in 1997. He is a part-time lecturer at George Washington University Law School, and a Research and Practice Associate of the Syracuse University Institute for National Security and Counterterrorism. He is the author of two books and several articles on law enforcement and intelligence issues.✠

The USA PATRIOT Act and Bilateral Information Sharing

Karl Sandoval
Trial Attorney
National Security Division

I. Introduction

Much has been written about the events leading up to the attacks of September 11, 2001, including the perceived inability of U.S. law enforcement agencies to disseminate information that was obtained about the hijackers before the attacks, in a timely, efficient, and thorough manner. Not surprisingly, the need to improve the intelligence sharing between domestic law enforcement agencies—and, by extension, with federal prosecutors—came squarely into focus in the aftermath of 9/11. Federal terrorism prosecutors, who were frustrated by the so-called "wall" observed between intelligence and law enforcement, joined in the call for a change. *See generally Hearing on the USA PATRIOT Act Before the House Subcommittee on Crime, Terrorism, and Homeland Security* (Apr. 19, 2005) (testimony of Barry M. Sabin, Chief, Counterterrorism Section, Department of Justice, concerning information sharing under the USA PATRIOT Act).

Congress moved quickly to address this problem. In late 2001, the USA PATRIOT Act, Pub. L. 107-56, 115 Stat. 272 (2001) (the PATRIOT Act), lifted long-standing barriers to information sharing by allowing the disclosure of grand jury information, and information derived from Title III activity, to any federal law enforcement official, where such information related to foreign intelligence or counterintelligence.

The Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135 (2002) (the HSA), and the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, 118 Stat. 3638 (2004) (IRTPA), expanded upon this foundation by allowing prosecutors and law enforcement agents to disclose to appropriate foreign government officials grand jury and Title III information involving a threat of domestic or international terrorism, for the purpose of responding to such a threat.

This article summarizes the statutory changes that have facilitated the bilateral sharing of grand jury and Title III information with foreign partners, and proposes that the ability to share terrorism-related information with them is especially crucial today, as terrorism increasingly plays out on an international stage. Indeed, terrorists routinely plan, coordinate, and seek to carry out their acts across oceans and entire continents. The disrupted plot to blow up airplanes flying from England to the United States during the summer of 2006 demonstrates the value of bilateral information sharing as a tool to prevent international terrorist attacks. To this end, Rule 6(e)(3)(D) of the Federal Rules of Criminal Procedure (the Rules) and 18 U.S.C. § 2517(8) now allow prosecutors and agents to share with their foreign counterparts, foreign intelligence and other terrorism-related information derived from grand jury and Title III activity. The evolution of these tools, and what they suggest about the ability of federal prosecutors to share terrorism-related information with their foreign counterparts, is discussed below.

II. The sharing of grand jury and Title III information before passage of The PATRIOT Act

Rule 6(e)(2) generally prohibits the disclosure of a "matters occurring before the grand jury," a term that is not defined in Rule 6 itself. However, the term "matters occurring before the grand jury" broadly encompasses "information that would reveal the strategy or direction of the investigation, the nature of the evidence produced before the grand jury, the views expressed by members of the grand jury, or anything else that actually occurred before the grand jury."

Rule 6(e)(2) codifies the traditional rule of grand jury secrecy by prohibiting members of the grand jury, government attorneys and their authorized assistants, and other grand jury personnel, from disclosing grand jury matters, subject to what were previously only a few exceptions in Rule 6(e)(3).

Prior to the passage of the PATRIOT Act and IRTPA, Rule 6(e)(3)(A) narrowly allowed for

disclosure only when it was made: (1) to a government attorney for use in the performance of the attorney's duty, and (2) to government personnel deemed necessary by a government attorney to assist in the performance of such attorney's duty to enforce federal criminal law. In addition, under Rule 6(e)(3)(C), disclosure could also be made to another federal grand jury, by court order and in other limited circumstances.

In practice, this chilled the ability of U.S. law enforcement agencies to share bilaterally (and with each other) intelligence information obtained during the course of a grand jury investigation. Indeed, in 2002, a report of the Select Committee on Intelligence observed that, in the ten years before 9/11, grand jury investigations of various terrorist plots had generated valuable intelligence, but little of it had been shared with the intelligence community. *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001,* S. REP. NO. 107-351 (2002), H.R. REP. NO. 107-792 at 89 (2002). While Rule 6(e) may have prevented the disclosure of some of the information, the Committee noted that Rule 6(e) increasingly came to be used simply as an excuse for not sharing information. *Id*. at 92.

Before the PATRIOT Act, 18 U.S.C. § 2517 also made it difficult for U.S. law enforcement agencies to disclose to one another information obtained from a Title III intercept. Section 2517 previously allowed disclosure of information derived from a Title III wiretap, for example, only in limited circumstances. As of September 11, 2001, Paragraph (1) of the statute provided as follows:

> (1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

Section 2517(1) remains unchanged from the version that existed prior to the PATRIOT Act.

The practical effect of this statute was to bar the bilateral (and domestic) sharing of terrorism-related information obtained from Title III activity, especially in those investigations where foreign officials were not already involved, which is the case in most Title III investigations.

III. Grand jury and Title III information involving foreign intelligence may now be shared

A. Grand jury information

Section 203(a) of the PATRIOT Act amended Rule 6(e)(3)(C) to allow grand jury matters "involv[ing] foreign intelligence or counterintelligence (as defined in Section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information," to be disclosed to any federal law enforcement, intelligence, protective, immigration, national defense, or national security official, to assist in the performance of their official duties. While the PATRIOT Act amended the then-existing version of Rule 6(e)(3)(C), these changes are now contained in Rule 6(e)(3)(D). The term "foreign intelligence information" was defined in Rule 6(e)(3)(C)(iv), now codified at Rule 6(e)(3)(D)(iii), to include information relating to the ability of the United States to protect against actual or potential attacks or other grave hostile acts, international terrorism, or information with respect to a foreign power or foreign territory that relates to the national defense or security of the United States. Under this section, a government attorney is also required to file, under seal, a notice with the court, advising it of the disclosure and identifying the departments, agencies, or entities, to which the disclosure was made. FED. R. CR. P. 6(e)(3)(D)(ii). Any federal official who receives information pursuant to this section may use that information only as necessary in the conduct of that person's official duties, subject to any limitations on the unauthorized disclosure of such information. FED. R. CR. P. 6(e)(3)(D)(i).

IRTPA expanded the exceptions to the general rule of grand jury secrecy, most notably with the creation of new Rule 6(e)(3)(D), which continues the PATRIOT Act's earlier changes. Rule 6(e)(3)(D) allows a government attorney to disclose any grand jury matter involving a threat of attack or other grave hostile acts of a foreign power, or a threat of domestic or international terrorism, to any appropriate foreign government official, for the purpose of preventing or responding to such a threat or acts. Congress previously sought to expand the exceptions to grand jury secrecy in the HSA. For example, § 895 of the HSA would have allowed disclosure

of grand jury matters to foreign governments in a number of circumstances. The Supreme Court, however, amended Rule 6 on April 29, 2002, making § 895 incapable of execution because it did not reference the then-current version of Rule 6. Therefore, Congress reenacted the changes contemplated by § 895 in IRTPA. An excellent analysis of the IRTPA amendments was provided by Arnie Celnicker, *Changes To Grand Jury Secrecy Made By The Intelligence Reform And Terrorism Prevention Act,* 54 UNITED STATES ATTORNEYS' BULLETIN 7 (2005).

IRTPA also amended Rule 6(e)(3) to allow disclosure of grand jury matters to a foreign government when disclosure is deemed necessary by a government attorney to assist in enforcing federal law, and when a government attorney seeks a court order for disclosure to a foreign government for its criminal investigation. FED R. CR. P. 6(e)(3)(A)(ii), 6(e)(3(E)(iii).

Thus, as it now stands, Rule 6(e)(3)(D) and, to a lesser extent, Rule 6(a)(3)(E), give prosecutors and agents considerable leeway to share grand jury information with foreign partners in cases involving terrorism and other threats to national security, subject to certain usage restrictions imposed upon the recipient. In part, Rule 6(e)(3)(D) now provides:

> (D) An attorney for the government may disclose any grand jury matter involving foreign intelligence, counterintelligence (as defined in 50 U.S.C. § 401a), or foreign intelligence information (as defined in Rule 6(e)(3)(D)(iii)) to any federal law enforcement, intelligence . . . or national security official to assist the official receiving the information in the performance of that official's duties. An attorney for the government may also disclose any grand jury matter involving, within the United States or elsewhere, a threat of attack or other grave hostile acts of a foreign power or its agent, a threat of domestic or international sabotage or terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by its agent, to any appropriate Federal, State . . . or foreign government official, for the purpose of preventing or responding to such threat or activities.

As noted above, an official who receives information under Rule 6(e)(3)(D) may use the information only as necessary in the conduct of that person's duties, subject to any limitations on the unauthorized disclosure of such information. Any foreign government official who receives such information may use the information only in a manner consistent with any guidelines issued jointly by the Attorney General and the Director of National Intelligence. FED. R. CR. P. 6(e)(3)(D)(i).

B. Title III information

Mirroring the new rules regarding the sharing of grand jury information, § 2517 was amended to allow disclosure of foreign intelligence information, obtained through Title III activity, to other federal law enforcement officials. Paragraph (6) of § 2517, which was added under the § 203(B) of the PATRIOT Act, provides:

> (6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information [as defined in 18 U.S.C. 2510(19)], to assist the official who is to receive that information in the performance of his official duties. Any federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

The definition of "foreign intelligence information" in 18 U.S.C. § 2510(19) is identical in substance to the definition of that term in former Rule 6(e)(3)(C)(iv), now codified at Rule 6(e)(3)(D)(iii).

Section 2517 was supplemented a year later, pursuant to the HSA, with the addition of paragraph (7), which authorizes disclosure of Title III information

> to a foreign investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or

> receiving the disclosure, and foreign investigative or law enforcement officers may use or disclose such [information] to the extent such use or disclosure is appropriate to the proper performance of their official duties.

More importantly, the HSA also added 18 U.S.C. § 2517(8), which allows law enforcement to disclose to foreign government officials Title III-derived evidence of a threat of actual or potential terrorism anywhere in the world. Section 2517(8) provides, in relevant part:

> (8) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to any . . . foreign government official to the extent that such contents or derivative evidence reveals a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, . . . [or] domestic or international terrorism . . . within the United States or elsewhere, for the purpose of preventing or responding to such a threat.

Just as with grand jury information received under Federal Rule 6(e)(3)(D), any foreign official who receives information pursuant to Paragraph (8) may use that information only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue.

18 U.S.C. § 2517(8).

IV. Conclusion

Terrorism is, by many accounts, the greatest long-term threat to the domestic safety and security of the United States. It is clearly a law enforcement issue. At the same time, the threat of terrorism also plagues many of America's most valued foreign partners. Almost every day, we learn of some new terrorist plot aimed at striking the United States or one of its partners. Indeed, the very nature of international terrorism is to operate across national borders and engage in increasingly complex, multilayered activities to strike globally.

The rules described above provide prosecutors and agents with valuable tools to fight terrorism by facilitating bilateral information sharing. Under Rule 6(e)(3)(D), a federal prosecutor may now disclose *any* grand jury matter involving a threat of terrorism to *any* appropriate foreign government official, for the purpose of preventing or responding to such a threat. The threat may be of domestic or international terrorism, and the act of terrorism may be directed against the United States or elsewhere. The threat need not be imminent or specific. Also, under Rule 6(e)(3)(D), no court order is required to make such a disclosure. Section 2517(8) is almost identical in substance, as it relates to information obtained from Title III activity.

While foreign government recipients of information under Rule 6(e)(3)(D) and 18 U.S.C. § 2517(8) are bound by certain limitations on their use of the information, the potential value of these provisions cannot be overstated. For example, if a federal grand jury witness testified that persons in the Middle East had a nascent plan to bomb a major European airport, a prosecutor could communicate that threat information to any appropriate foreign government official, for the purpose of preventing or responding to the threat. The prosecutor would need to timely provide notice of the disclosure to the court in the district where the grand jury was convened, but the provision of the information on a bilateral, or even multilateral, basis could be easily accomplished. The result would be the same if the "threat information" was obtained by authorized Title III means.

Frequently, prosecutors and law enforcement agents neglect to take advantage of these provisions, often because they are simply unaware of their existence or the extent to which they may facilitate the effective dissemination of threat-based intelligence. In order to ensure that such foreign intelligence information is shared with foreign partners in the fight against terrorism, prosecutors and agents are encouraged to enlist the aid of Rule 6(e)(3)(D) and 18 U.S.C. § 2517(8), as well as the expertise of prosecutors in the Counterterrorism Section of the National Security Division. As with any international criminal law issues, U.S. prosecutors should also coordinate information-sharing with the Criminal Division's Office of International Affairs.❖

ABOUT THE AUTHOR

❑**Karl Sandoval** is a Trial Attorney in the Terrorist Financing Unit of the Counterterrorism Section, National Security Division. He was an

Assistant U.S. Attorney for the Southern District of California before joining the Counterterrorism Section in 2006. Mr. Sandoval was in private civil practice for ten years before joining the U.S. Attorney's Office in 2004.✠

Obtaining Foreign Evidence Outside of the Mutual Legal Assistance Treaty Process

Corey J. Smith
Antiterrorism Advisory Counsel Regional Coordinator
Counterterrorism Section
National Security Division

I. Introduction

One of the few truisms in litigation, criminal and otherwise, is that a case is only as good as its (admissible) evidence. As technology shrinks the world, prosecutors increasingly find themselves handling international criminal cases that present new evidentiary challenges. Whether an international tax shelter case, Racketeering Influenced Corrupt Organization (RICO), or terrorist financing prosecution, foreign evidence increasingly comprises a large part of the government's case-in-chief. Obtaining evidence from foreign jurisdictions is only the first of many hurdles that the prosecutor must overcome. In addition, the prosecutor must also authenticate the evidence under Federal Rule of Evidence 901, and often, overcome inherent hearsay.

If the prosecutor is fortunate, the situs of the foreign evidence is a country with which the United States has a Mutual Legal Assistance Treaty (MLAT). If the treaty encompasses the crimes which the prosecutor is contemplating, evidence acquisition may be relatively straightforward; a simple treaty request to the foreign government may suffice. If, however, an MLAT does not exist, or the contemplated charges are not covered under the treaty, alternative methods must be employed. For instance, the United States Government has MLATs with many Caribbean countries, few of which encompass Title 26 offenses. In these instances, there is a panoply of tools available, each escalating in its intrusiveness.

A formal government-to-government request for assistance, or Letters Rogatory, is the most well-known method of obtaining foreign evidence outside of an MLAT. As an alternative, the prosecutor may inquire if law enforcement has a pre-existing or Simultaneous Criminal Investigation Program arrangement with the law enforcement authorities in the foreign jurisdiction. Alternatively, the prosecutor may seek evidence under the procedures available in the legal system of the foreign country. If the third party possessor of the evidence has a presence in the United States, a Bank of Nova Scotia (BNS) or PATRIOT Act subpoena may be appropriate. Finally, under particular circumstances, the prosecutor may simply move to compel the United States person with signatory authority over the evidence in question to consent to its production. The methodology to employ is dictated by the unique circumstances of each investigation and the legal environment of the foreign country in question. The most efficient way to evaluate the legal climate of the foreign jurisdiction at play is through consultation with the Department of Justice's (Department) Office of International Affairs.

II. The Simultaneous Criminal Investigation Program

The United States does not have a Simultaneous Criminal Investigation Program (SCIP) arrangement with many foreign countries. A SCIP is a formal, nonjudicial arrangement between complimentary law enforcement agencies in two countries to share evidence. The best known SCIP is between the Internal Revenue Service (IRS), Criminal Investigation Division (CID), and its counterpart, the Canadian Department of National Revue, Canadian Customs and Revenue Agency (CCRA). This agreement was executed by the United States and Canadian Governments on March 31, 1983, and reauthorized on May 3, 2001.

The agreement permits the IRS-CID to share tax return information with CCRA agents under Title 26 U.S.C. § 6103(k)(4), if such sharing will further the development of an ongoing criminal tax investigation in the United States. The SCIP agreement, however, is limited. Paragraph 6 of the SCIP only permits sharing of evidence if such disclosures further the ends of "tax administration." The SCIP process cannot be used to obtain evidence in Title 18 investigations. Moreover, "matters occurring before the Grand Jury" cannot be shared under the SCIP process. Another concern with law enforcement-to-law enforcement evidence sharing is general secrecy. In many instances, security in foreign jurisdictions is not as reliable as in the United States law enforcement community. Occasionally a foreign law enforcement agency may be willing to share evidence with the United States without requesting reciprocity, but more often than not, the one way street of evidence sharing turns out to be a dead end.

III. The Letters Rogatory

A Letters Rogatory, in contrast to a SCIP or MLAT, is a judicial animal that issues from the court. It is a formal request from a United States District Court to the judiciary of a foreign nation, requesting the assistance of the latter in obtaining evidence. The execution of a request for judicial assistance is based on comity between nations at peace. *See United States v. Zabady*, 546 F. Supp 35, 39 n.9 (M.D. Pa. 1982). The power of United States federal courts to issue Letters Rogatory derives from Title 28 U.S.C. § 1781 and from the courts' inherent authority. *United States v. Reagan*, 453 F.2d 165, 171-73 (6th Cir. 1971); *United States v. Staples*, 256 F.2d 290 (9th Cir. 1958); *United States v. Strong*, 608 F. Supp. 188, 192-94 (E.D. Pa. 1985); *B & L Drilling Electric v. Totco*, 87 F.R.D. 543, 545 (W.D. Okla. 1978). Federal courts also possess the power to execute Letters Rogatory at the request of foreign tribunals. 28 U.S.C. § 1782; *In Re Request for Assistance from Ministry of Legal Affairs of Trinidad and Tobago*, 648 F. Supp 464 (S.D. Fla. 1986).

Evidence, including documents and the testimony of witnesses, may properly be sought by means of a request for foreign judicial assistance before or after formal charges have been brought. *United States v. Reagan*, 453 F.2d at 173 n.4; In Re Grand Jury 81-2, 550 F.Supp 24, 29 (W.D. Mich. 1982); *United States v. Strong*, 608 F.Supp at 194. The request for assistance may also include the execution of a search warrant. Such a search will be upheld if executed in accordance with the laws of the country in which the search took place, as long as the country has reasonable procedural protections and safeguards consistent with United States law. *United States v. Barona*, 56 F.3d 1087 (9th Cir. 1995).

A prosecutor wishing to employ the use of a Letters Rogatory must first obtain the approval of the Office of International Affairs (OIA). The OIA will have an attorney assigned to the country from which evidence is sought, and he or she will be able to inform the prosecutor of the particular legal landscape of that country. Once OIA approval is obtained, the prosecutor must prepare a motion for the court and the actual Letters Rogatory, which must include the charges being investigated, the elements of those charges, the criminal conduct being investigated, and a precise description of the evidence sought. If any specific evidence gathering techniques, such as witness questioning, are also being sought, that technique must also be described. Most importantly, the prosecutor must describe how the evidence sought will assist in proving the criminality of the targeted suspect. The affiant in this case is not the special agent, but the prosecutor.

The Federal Rules of Criminal Procedure are silent as to the procedure for the issuance of Letters Rogatory, but case law suggests that applications may be made *ex parte*. If the evidence being sought is for investigative purposes only, authentication of the evidence under Federal Rule of Evidence 901 is not a concern. If, however, the evidence is sought for

preservation and use at trial, such as bank records or statements of witnesses, the domestic evidentiary rules must be observed. For instance, if a request for foreign judicial assistance seeks testimony for use at trial, the requirements of Rule 15 of the Federal Rules of Criminal Procedure must be followed. *See United States v. Strong*, 608 F. Supp at 192-94 (approving post-indictment request for judicial assistance to obtain deposition of foreign witness). If foreign bank records are being sought, the requirements of 18 U.S.C. § 3505, including notice, must be followed.

Even if a foreign court accepts a United States Letters Rogatory, and issues an order compelling the production of the requested evidence, it is by no means certain that the United States prosecutor will receive the evidence in question, or will receive it in a form admissible at trial. Depending on the country, the foreign prosecutors charged with enforcing the Letters Rogatory Order may be unwilling to enforce the foreign Order, or the third party possessor of the evidence may simply refuse to comply. Systemic corruption in foreign jurisdictions is only one reason why compliance with a Letters Rogatory may be problematic. There are many less nefarious reasons why requested foreign evidence may never be produced through a Letters Rogatory.

IV. Bank secrecy laws suspension

Bank secrecy laws are the obstacle most frequently encountered by United States prosecutors when seeking foreign financial records. Many jurisdictions have made it a crime for financial institutions to provide customer bank records to law enforcement, or to foreign law enforcement. Many of these countries, however, have exceptions to these laws. For instance, the Turks and Caicos Islands can provide bank records if the investigation does not involve tax charges. Some jurisdictions provide a procedure through which law enforcement, including foreign law enforcement, can apply for a suspension of the bank secrecy laws. For example, in Lebanon, Law 318 of the Lebanese Republic, Article 6, creates a *Special Investigation Commission* which is empowered to lift Lebanese bank secrecy laws in particular money laundering investigations. Law 318, Article 1, enumerates the types of investigations in which the bank secrecy laws can be suspended. Under Law 318, the Lebanese bank secrecy laws can be suspended only in cases involving the following.

- The growing, manufacture, or trading of narcotics.
- Organized crime investigations.
- Terrorist acts.
- Illegal arms trade.
- Stealing or embezzling public or private funds, or their appropriation by fraud.
- Counterfeiting money or official documents.

Of course, the prosecutor must be mindful of the political environment of the requested country. A procedure like that codified in Law 318 is only as good as the will to enforce it.

The best way for a prosecutor to ascertain if a procedure like Law 318 is available in a particular jurisdiction is to contact counsel for the financial institution from which records are sought. Typically, counsel will work with the United States prosecutor to achieve a mutually advantageous resolution to obtaining foreign evidence. Counsel's objective is not to thwart law enforcement, but to satisfy it. If the financial institution's counsel has any experience in the area of criminal law and foreign evidence gathering, he or she will be motivated to prevent their client from being on the receiving end of a more intrusive request for evidence, such as a BNS or PATRIOT Act Subpoena.

A. Bank of Nova Scotia subpoena

If an evaluation of the facts and circumstances of a particular case cause a prosecutor, in consultation with OIA, to conclude that a Letters Rogatory or Bank Secrecy Act (BSA) exception request are not likely to succeed, and if the financial institution in question has a presence in the United States, a BNS or PATRIOT Act subpoena may be appropriate. Institutions that maintain branches or affiliates in the United States are subject to legal process. *In Re Grand jury Proceeding (Bank of Nova Scotia)*, 722 F.2d 657 (11th Cir. 1983), *appeal following remand*, 740 F.2d 817 (1984); *In Re Grand jury Proceeding (Bank of Nova Scotia)*, 691 F.2d 1384 (11th Cir. 1982). If the financial institution does not maintain a branch or affiliate in the United States, but has a correspondent relationship with a United States bank, a PATRIOT Act Subpoena may be appropriate. 31 U.S.C. § 5318(k)(3).

OIA approval is required for the issuance, and if necessary, the enforcement, of all BNS subpoenas. *See* USAM 9-13.525; Criminal

Resource Manual, § 279. Approval of a BNS subpoena is dependent on a number of factors.

- The availability of alternative methods for obtaining the records in a timely manner.
- The indispensability of the records to the success of the investigation or prosecution.
- The need to protect against the destruction of records located abroad and to protect the United States' ability to prosecute for contempt or obstruction of justice for such destruction.

If enforcement is necessary, the prosecutor will need to plead a so-called comity analysis, and the Court will be required to balance international comity against law enforcement needs to determine if an enforcement order should issue. Comity analysis derives from § 442(1)(c) of the Restatement (Third) of the Foreign Relations Law of the United States (1987). *See Richmark Corp v. Timber Falling Consultants*, 959 F.2d 1468, 1474-79 (9th Cir. 1992). Typically, enforcement takes the form of daily fines until compliance is obtained. Service of a BNS subpoena is upon a financial institution's United States branch or U.S. registered agent. If the foreign bank does not have a branch or affiliate in the United States, and other means of obtaining the records are not viable, the only remaining alternative may be a PATRIOT Act subpoena.

B. The PATRIOT Act subpoena

The Patriot Act subpoena derives its name, obviously, from the recently enacted PATRIOT Act, but is codified at 32 U.S.C. § 5318(k)(3), which states:

> The Attorney General may issue … a subpoena to any foreign bank that maintains a correspondent account in the United States and requests records related to such correspondent account, including records maintained outside of the United State relating to the deposit of funds in the foreign bank

Much like a BNS subpoena, a prosecutor must obtain OIA approval prior to issuing and/or enforcing a PATRIOT Act subpoena. To obtain approval, the prosecutor must establish an extraordinary need for the subject evidence, and show that no other method is likely to result in compliance. In counterterrorism or counterespionage cases, a classified supplement can be submitted as part of the approval package. In most cases, by the time the prosecutor is contemplating the use of a BNS or PATRIOT Act subpoena, he or she has had discussions with bank counsel. It is often likely that the prospect of a PATRIOT Act subpoena will encourage a foreign financial institution to agree to some alternative method of providing the requested records, short of a subpoena, that will not violate the subject jurisdiction's bank secrecy laws. Voluntary consent is one such alternative procedure.

V. Compelled consent order

If the party controlling a foreign bank account is subject to United States' jurisdiction or process, prosecutors can seek a court order compelling an account holder to sign a consent form obliging the foreign institution to provide the records in question. *Doe v. United States*, 487 U.S. 201 (1988); *United States v. Ghidoni*, 732 F.2d 814 (11th Cir. 1984); *United States v. Lehder-Rivas*, 827 F.2d 682 (11th Cir. 1987). The Supreme Court has ruled that such an order, if the consent form is properly worded in the hypothetical, does not violate a signatory's Fifth Amendment privilege against self-incrimination. *Doe v. United States*, 487 U.S. at 206-18. The consent form must clearly state that the signatory is not affirming the existence or control over records that may be located at a particular institution, but that inasmuch as the institution requires his consent for the release of any records in its possession, such consent is given. If a nominal custodian, or signatory, refuses to voluntarily sign such a consent form, the prosecutor can move the applicable court for an order compelling consent. *See id.* The Supreme Court held in *Doe* that, since a properly worded hypothetical consent form does not implicate the signatory's Fifth Amendment rights, the signatory can be compelled to provide said consent. The underpinning for this result is the precept that, in the interest of the public welfare, the government is entitled to everyone's evidence. Why should access to the sought-after financial records be denied simply because of the unfortunate happenstance that they are located outside the United States? This argument is especially poignant when the person, under whose name these records are being held, is subject to U.S. jurisdiction.

Foreign courts have had mixed reactions to these directives. A court in the Cayman Islands, a dependency of the United Kingdom, held that such compelled disclosure directives do not constitute voluntary and freely given consent for

disclosure, as required under the secrecy laws of that jurisdiction. *In re ABC Ltd*., 1984 CILR 130, 134-45 (Grand Court of the Cayman Islands, 1984). For other countries that do not have such stringent secrecy statutes, and that follow British common law, there is authority that such disclosures do constitute valid consent under the common law duty of a banker to keep the financial affairs of clients private. *Tournier v. National Provincial & Union Bank of England*, 1 K.B. 461 (1924).

The use of compelled consent orders has been widely successful in obtaining foreign bank records. Even when the account holder is located outside the United States, the prospect of a subpoena or compelled consent order may lead a General Counsel for a foreign financial institution to assist in obtaining voluntary consent under these procedures. Also, there is no reason why a compelled consent order cannot be used to obtain other types of records that are subject to the secrecy provisions of foreign jurisdictions, for example, accounting records.

It is important for prosecutors to remember one of the foundational dictates of the noble profession, regardless of the methodology employed in obtaining foreign evidence. "Everything is negotiable." Before a prosecutor uses a PATRIOT Act subpoena, it is not only required, but wise, to explore less intrusive, and more informal, methods of obtaining the requested evidence. More often than not, bank's counsel will be a willing and capable ally in this endeavor. If compulsory process is required, approval will be easier to obtain if it is preceded by a record of informal request and negotiation.❖

ABOUT THE AUTHOR

❑**Corey Smith** is an Antiterrorism Advisory Counsel Regional Coordinator with the National Security Division, Counterterrorism Section. He previously served as Assistant Chief with the Tax Division, Southern Criminal Enforcement Section.

Material contained within this article derived, in part, from material authored by James Springer, Senior Litigation Counsel, Tax Division, retired.

National Security Evidence and Terrorism Prosecutions: Cooperation Between the United States and the United Kingdom

Jocelyn A. Aqua
Trial Attorney
Counterterrorism Section
National Security Division

I. Introduction

On the morning of August 10, 2006, British Home Secretary John Reid announced that British authorities had arrested twenty-one individuals, in order to disrupt an international terrorist plot involving a series of simultaneous attacks designed to detonate liquid explosives on board aircraft traveling from the United Kingdom to the United States. By August 11, 2006, three additional people were arrested and the assets of nineteen of those arrested were frozen by the Bank of England. As acknowledged by Prime Minister Tony Blair, the events leading up to the arrests were a result of "an enormous amount of cooperation with the U.S. authorities which has been of great value" to the investigation. *"Airlines Terror Plot" Disrupted* (BBC News Aug. 10, 2006), *available at* http://news.bbc.co.uk/2/hi/uk_news/4778575.stm.

Within hours of this public announcement, Homeland Security Secretary Michael Chertoff, United States Attorney General Alberto Gonzales, Federal Bureau of Investigation (FBI) Director Robert Mueller, and Assistant Secretary for the Transportation Security Administration Kip Hawley, held a joint press conference to discuss the threat, highlighting the strong counterterrorism partnership between the United States and the United Kingdom. "From the beginning of the investigation, we have been in constant contact with our counterparts in the U.K. We share the same philosophy of prevention, a sense of urgency to dismantle these terrorist cells before an attack occurs. The FBI and other law enforcement intelligence agencies have worked closely with our colleagues at MI-5 on all aspects of this case, and they have aggressively pursued every domestic lead that has arisen from the intelligence that led to these arrests." Press Release, Department of Homeland Security Briefing on U.K. Terror Arrests (Aug. 10, 2006). Attorney General Gonzales, in a speech the following week, emphasized the long-standing and robust policies in place for sharing national security information at all levels of government, noting that "[t]he level of cooperation between the United States and our foreign [U.K.] counterparts is outstanding and is truly the untold story of the war on terror." Attorney General Alberto R. Gonzales, Prepared Remarks at the World Affairs Council of Pittsburgh on Stopping Terrorists Before They Strike: The Justice Department's Power of Prevention (Aug. 16, 2006).

Although the United Kingdom and the United States have secured unprecedented new levels of cooperation between the U.S. and U.K. criminal justice systems, this most recently foiled terrorist plot draws attention to the significant differences in the way United States and British authorities investigate and prosecute terrorism cases. The British enjoy certain advantages under their antiterrorism laws, including: broader arrest and detention powers, lower necessity standards for intercepting communications, and more comprehensive laws criminalizing the encouragement or incitement of terrorist acts. However, in addition to the many effective counterterrorism-related investigative tools available to U.S. law enforcement, U.S. prosecutors also possess a greater ability to use domestically intercepted communications as evidence, which has been critical to the success of the United States in extracting guilty pleas and obtaining terrorism convictions.

Counterterrorism prosecutions are considered by both countries to be an essential tool for disrupting terrorist operatives. As such, this article discusses the following topics:

- The advantages and disadvantages of the antiterrorism-related laws used in counterterrorism investigations and prosecutions in the United Kingdom, including evidentiary problems associated with the current U.K. prohibition on the use of certain U.K.-intercepted communications in terrorism prosecutions.
- Recent examples of national security intelligence sharing between U.S. and U.K. law enforcement that has resulted in successful terrorism prosecutions in both countries.
- Further guidance for U.S. and U.K. prosecutors regarding early information sharing in serious and complex criminal cases, including counterterrorism cases, in order to determine the most appropriate venue for prosecution.

II. Arrest and detention powers in the United Kingdom

Police in the United Kingdom are an integral part of counterterrorism enforcement and have been given broad authority to stop and search a vehicle or pedestrian on the grounds of preventing terrorism. *See* Terrorism Act 2000, §§ 43- 44. (The U.K. statutory laws and accompanying explanatory notes discussed herein are all available at http://www.opsi.gov.uk/legislation/uk.htm.) Additionally, U.K. police have preemptive power to arrest an individual, without a warrant, when there is a "reasonable suspicion" that the individual has been involved in the preparation, instigation, or commission of an act of terrorism, regardless of whether the police believe the suspect is committing or has committed a crime. *See id*. § 41. A "reasonable suspicion" standard in the United Kingdom generally will not meet the "probable cause" standard required pursuant to the Fourth Amendment, although U.K. police often rely upon intercepted communications as grounds for "reasonable suspicion."

The British Government also may issue control orders, which are preventative measures to restrict individuals who are believed to pose a threat to national security, but where there is insufficient evidence to bring them to trial. Prevention of Terrorism Act 2005, §§ 1-9. The orders require judicial approval, at times valid up to one year, and may restrict or ban an individual's freedom to travel, to meet with certain groups, to visit certain locations, or to use cell phones or the Internet. Additionally, certain control orders may even require a suspect to be monitored by electronic tagging. As will be discussed below, one of the primary benefits of control orders has been the ability to limit a suspect's opportunity to commit terrorist acts, while U.K. law enforcement continues to collect evidence that is admissible in a British court of law.

Control orders thus can impose burdensome restrictions on a suspect's civil liberties, and do not allow the individual the right to be present in a hearing or review the evidence on which the order is based. For these reasons, control orders have been challenged in British courts as being incompatible with the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), which was incorporated into British domestic law in 1998 through the U.K.'s Human Rights Act. Article 5 of the ECHR provides: "Everyone who is deprived of his liberty by arrest or detention shall be entitled to take proceedings by which the lawfulness of his detention shall be decided speedily by a court and his release ordered if the detention is not lawful." However, British courts do not have the power to overturn a statute that is found by the courts to be inconsistent with the ECHR; the courts can only make a declaration of incompatibility. Human Rights Act, § 4, *available at* http://www.hri.org/docs/ECHR50.html. The U.S. Attorney General has noted that the First Amendment's protections of freedom to travel and associate generally make control orders incompatible with U.S. law. *See* Alberto R. Gonzales, U.S. Attorney General, Prepared Remarks at the Vienna E.U. Interior Ministers Conference (May 5, 2006).

A more recent addition to the United Kingdom's detention powers permits the British Government to detain a terrorist without criminal charges for up to twenty-eight days before the suspect must be charged with a crime or released. Judicial approval is necessary after forty-eight hours and again after seven days. Terrorism Act of 2006, § 23-24. The judge, however, does not need to find probable cause–only that there are "reasonable grounds for believing that the further detention of the person to whom the application relates is necessary to obtain relevant evidence whether by questioning him or otherwise or to preserve relevant evidence." *Id*. This allows more time for U.K. prosecutors to gather evidence before formally charging a terrorism suspect, and,

of course, differs from U.S. law, which requires U.S. prosecutors, typically, to file a complaint establishing probable cause within forty-eight hours of a warrantless arrest. Suspects held in connection with the August 2006 airline plot were the first individuals detained under the U.K. law for longer than two weeks.

III. Collection of evidence in the United Kingdom

The prevailing law governing the acquisition of evidence within the United Kingdom, including the interception of communications by the law enforcement, security, and intelligence agencies, is the Regulation of Investigatory Powers Act of 2000 (RIPA). RIPA regulates interceptions of any communication made via the public mail, a public telecommunications system (phone and Internet), or a private telecommunications system (internal phone system or computer network). RIPA, §§ 1-2. RIPA also applies to communications that are being stored "in a manner that enables the recipient to collect it or otherwise to have access to it." *See* RIPA Explanatory Notes, ¶ 32.

Intercepted communications include not only the covert interception of telephone calls, but also E-mails, faxes, text messages, Voice over Internet Protocol (VoIP), and ordinary mail. *Id.* § 2. As will be discussed in detail below, RIPA prohibits the use of such intercepted information as evidence in prosecutions. *Id.* § 17.

RIPA also describes the circumstances in which the acquisition of electronic communications can lawfully take place without a warrant, such as: when there are reasonable grounds to believe that both parties have consented (notification that the call will be recorded); with the consent of one party (where one party is an undercover agent); where the interception takes place on an internal network with the consent of the controller of the system in connection with the operation of service; when the interception occurs in certain hospitals and in prisons. *Id.* §§ 3(1)-(3), 4(4)-(6).

Additionally, RIPA regulates the collection of other communications and information, including: information obtained covertly pursuant to a physical search or audio/video surveillance authorized on a residence or private vehicle using an electronic bugging device ("intrusive surveillance"); the collection of private data or other information, or the collection of information through the use of electronic bugging in public places, such as work areas and in public vehicles ("directed surveillance"); the use of covert human intelligence or undercover sources; and noncontent data collection such as telephone records, Internet Service Provider records, and subscriber information. *Id.* §§ 21-32. The levels of authorization that must be obtained, and the circumstances under which public authorities may authorize these types of information gathering vary, depending on the intrusiveness of the collection and the entity undertaking the collection.

Although the term "intercept evidence" is sometimes confused with the information acquired through the covert methods described above, there is no absolute bar on the use of information legally obtained, without a warrant or through electronic bugging, as evidence in a British or foreign criminal proceeding.

There are several major differences between U.K. and U.S. wiretap authorities. First, in the United Kingdom, an interception warrant is authorized through executive act by the Home Secretary instead of through judicial approval. *Id.* § 5. Separation of powers issues are less of a concern in the United Kingdom under the parliamentary system, where the Prime Minister and his cabinet also sit as members of the legislature. Thus, there is only retrospective judicial oversight by an Interception of Communications Commissioner, who provides an annual review, and by the Investigatory Powers Tribunal, which hears cases brought by aggrieved persons. *Id.* §§ 57, 65-69.

Additionally, British interception warrants are granted under a "necessity" and "proportionality" standard, as opposed to the "probable cause" standard required under U.S. law. The British warrant must be necessary under one of the following circumstances.

- In the interests of national security.
- For the purpose of preventing or detecting a serious crime.
- For safeguarding the economic well-being of the United Kingdom.
- For giving effect to the provisions of any international mutual assistance agreement in circumstances appearing to the Home Secretary to be equivalent to those in which he would issue a warrant.

Id. § 5(3)(a)-(d). An interception warrant also must be proportionate in that the Home Secretary must balance the intrusiveness of the interference against the need for it in operational terms, and consider whether the information which is sought could reasonably be obtained by other means.

U.S. criminal and intelligence electronic surveillance authorities also contain "necessity" provisions that require a court to find that the information sought is not available through normal investigative procedures. *See* Title III of the Omnibus Crime Control and Safe Streets Act 1968, 18 U.S.C. § 2518(3)(3); Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. §§ 1804(a)(7)(E)(ii), 1823(a)(7)(C). Additionally, FISA also requires that a high-level Executive Branch official certify the same. 50 U.S.C. §§ 1804(a)(7),1823(a)(7).

The necessary finding of probable cause, required under both U.S. statutes, would seem to be a more stringent legal standard than a necessary and proportionate standard. To obtain a federal criminal wiretap, a United States judge must also find that there is probable cause to believe that an individual is committing, has committed, or is about to commit, an enumerated federal crime; that communications relating to the crime will be obtained through the interception; and that the targeted facilities or location are being, or will be, used in connection with commission of the offense, or are leased to or commonly used by the targeted individual. 18 U.S.C. § 2518(3). To intercept communications or conduct a physical search of stored communications under FISA, a judge sitting on the Foreign Intelligence Surveillance Court must conclude, *inter alia*, that there is probable cause to believe that the target is a foreign power or an agent of a foreign power, and that the targeted facilities or locations are, or are about to be, used by a foreign power or agent of a foreign power (or for physical search authority, that the premises or property to be searched is owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power). *See* 50 U.S.C. §§ 1805(a)(3), 1824(a)(3). It is likely that the lower authorization standard for British interception warrants, as well as the lack of judicial approval, both contribute to the reluctance of the British government to amend RIPA and admit evidence from interception warrants in British courts of law.

Another significant difference is the lack of any notice provision in RIPA to require that the subject of an interception warrant be notified of the collection, as compared to FISA and Title III, which both have notice provisions. *See* 18 U.S.C. § 2518(8)(d) (notice to aggrieved party upon expiration unless delay obtained); 50 U.S.C. §§ 1806(c)-(d), 1825(d)-(e) (notice to aggrieved party if government intends to use FISA-obtained or derived information in a proceeding).

IV. Use of evidence in United Kingdom terrorism prosecutions

As mentioned above, RIPA precludes U.K. prosecutors from using information obtained through British interception warrants in a criminal proceeding, unlike Title III and FISA, which impose legal safeguards so that evidence secured pursuant to a lawful order may be admissible in court under certain conditions, notwithstanding other external evidentiary bars. In the United Kingdom, the general rule is that neither the possibility of interception, nor intercepted material itself, can play any part in legal proceedings. This excludes evidence, questioning, and assertion or disclosure in legal proceedings likely to reveal the existence (or the absence) of a warrant issued under the Act. The prohibition applies to protection of the contents of an intercepted communication or related communications data, if such disclosure could potentially reveal that surveillance occurred, and further protects any actions that might suggest that interception occurred. RIPA, § 17(1). There are exceptions for using intercepted communications, for example, in immigration proceedings and in appeals to terrorism designations, but the existence of the warrant or its contents are never disclosed to the defendant. *See* RIPA, §§ 18(1)(e)-(f) and (2).

The issue of whether to lift the ban has been studied and rejected several times by the British Government, and since August 2006 has been the subject of heated public debate. Various members of Parliament, Britain's current Attorney General, and the Metropolitan Police Commissioner, New Scotland Yard, all have publicly denounced the ban as an impediment to successful terrorism prosecutions. As a result, the Prime Minister has sought to reevaluate the government's prohibition once again. Ironically, both liberals and conservatives object to the prohibition. Several major human rights organizations strongly object

to the ban and have argued that the evidentiary difficulties espoused by the British Government to justify various exceptional counterterrorism measures imposed over the past six years are more violative of human rights than the use of classified evidence at trial. These statutorily created counterterrorism measures have included: the indefinite detainment of non-U.K. persons suspected of terrorist activity, which has since been found unlawful and has been repealed; the use of control orders, which also has been the subject of litigation; and the implementation of a precharge detention policy for up to twenty-eight days for those suspected of terrorist activity. All such measures were implemented, in large part, because of the inadmissibility of evidence from an interception warrant in criminal proceedings.

The British Government has concluded in the past that, despite the difficulties in acquiring evidence for terrorism prosecutions, the ban is necessary to prevent the exposure of British intercept techniques and capabilities, and to lift the ban would undermine intercept warrants as an effective crime fighting tool. Moreover, the British Government concluded that, under the requirements for a fair trial, the government would be required to record and retain all intercept material, which it is not currently required to do. This, according to the British Government, would overwhelm the already overburdened intelligence structure, impose intolerable resource burdens on intercepting agencies, and lead to a grave loss in capability. The British Government has noted that using intercept material in court might help convict some lower level criminals. However, it is of less value against the most serious offenders, such as terrorists, who are often the most security-conscious, particularly when it comes to communications. Currently, the United Kingdom is the only common law jurisdiction to prohibit the use of certain intercepted communications in criminal proceedings. It is not clear whether the upsurge in popular demand to reconsider the current policy will effect any change.

Notwithstanding the inadmissibility of certain intercepted communications in court, RIPA provides an exception for nonevidentiary disclosure to U.K. prosecutors to ensure fairness in criminal proceedings. *See* RIPA, § 18(7)(a). "Fairness" plays an important role in British prosecutions, as imported by Article 6 of the ECHR, which requires that there be a "fair and public" hearing, where the accused must be informed of the nature and the cause of the accusation. *See* RIPA Explanatory Note 5 ¶ 5. RIPA, however, requires that intercepted material be destroyed as soon as its retention is no longer necessary for a purpose authorized under the Act. RIPA, § 15(4). If the prosecutor concludes that the material affects the fairness of the proceedings, in the interests of justice, he may consult the trial judge in an *in camera, ex parte*-style review–an exceptional circumstance. *Id*. § 18(7)(b), (9). The judge, after having considered the intercepted material disclosed to him and determining that the information is essential, in the interest of justice, may direct the prosecution to make an admission of fact that is abstracted from the interception, but that does not reveal the fact of interception. Nothing in these provisions, however, allows intercepted material, or the fact of interception, to be disclosed to the defense.

Significantly, in the United Kingdom, there is no statutory bar on the use of foreign-intercepted communications obtained in accordance with foreign laws. Thus, it is possible for U.K. prosecutors, such as the Crown Prosecution Service (CPS), who are responsible for prosecuting terrorism cases in the United Kingdom, to use United States or other foreign -intercepted communications as evidence in their criminal proceedings. Evidentiary use of admissible information, including foreign evidence, is governed by rules of admissibility that emphasize relevance and fairness. The Police and Criminal Evidence Act of 1984 (PACE) allows the courts discretion to exclude otherwise admissible evidence if, having regard to the manner in which it was obtained, its admission would have such an adverse effect upon the fairness of the proceedings. PACE, § 78. This law could cause problems for U.K. prosecutors who would like to use information from foreign intercepts in court, such as those obtained pursuant to FISA, where the defendants in a British prosecution would not be permitted equal access to the information.

U.K. prosecutors are required to disclose to the defense all material that undermines the prosecution's case or assists the defense's case, in order to ensure the fairness of the criminal proceedings. However, where disclosure of material would, among other things, cause harm to national security, the prosecution may make a claim to the court for public interest immunity. Section 3(6) of the Criminal Procedure and Investigations Act 1996 (CPIA) prohibits a court

from disclosing to the defense any material that it concludes is not in the public interest. CPIA, § 3(6). British courts will decide *in camera* and *ex parte* whether the public interest in nondisclosure is outweighed by the public interest in the defendant having access to all relevant material. If the court rejects a claim for public interest immunity, the U.K. prosecutors may withdraw the prosecution to avoid having to make a damaging disclosure and to maintain the confidentiality of the information and the good relations between both governments. *See* Attorney General's Section 18 RIPA Prosecutors Intercept Guidelines, *available at* http://www.lslo.gov.uk/guidance/2003_RIPA_intercept_guide_Eng_Wales.doc; *see also* CPS Disclosure Manual on public interest immunity in criminal proceedings, *available at* http://www.cps.gov.uk/legal/section20/chapter_a.html.

V. Use of British evidence in U.S. courts

The United Kingdom's 2001 Anti-terrorism, Crime and Security Act (ATCSA) was enacted following 9/11, and allows for the disclosure of confidential information obtained by U.K. government entities to assist in criminal investigations or proceedings, either in the United Kingdom or abroad. ATCSA, § 18. Under this statute, the Home Secretary has the discretion to permit the use of such information in foreign courts and to determine whether it is necessary to require restrictions on the disclosure and use before approving its dissemination. The Home Secretary may prevent disclosure to foreign jurisdictions that do not offer an "adequate" level of protection, or for other policy reasons, including that it would be more appropriate for the United Kingdom to exercise jurisdiction.

With regard to U.K.-intercepted communications, RIPA states that there should be "restrictions [ ] in force which would prevent, to such extent (if any) as the Secretary of State thinks fit, the doing of anything in, for the purposes of, or in connection with, any proceedings outside the United Kingdom which would result in such a disclosure [that] could not be made in the United Kingdom." RIPA, § 15(7)(b). The Home Secretary thus generally prohibits foreign governments from using British intercept evidence in criminal proceedings, including terrorism prosecutions. However, a frequently cited independent review conducted by members of parliament (the Newton Committee) submitted to the Home Secretary in December 2003, per requirement of ATCSA, concluded that the ban on the use of intercept evidence did not apply to the use of the same evidence in foreign courts, "assuming that the intelligence and security services are prepared to provide them." *See* Report of the Privy Counsellors Review of the Anti-Terrorism Crime and Security Act 2001 (the Newton Committee) (HC 100, Dec. 18, 2003), ¶ 210, *available at* http://www.statewatch.org/news/2003/dec/atcsReport.pdf.

VI. National Security information sharing between U.S. and U.K. law enforcement

The massive counterterrorism investigation associated with this latest airline threat has resulted in the acquisition of monolithic amounts of data, amassed both before and since the arrests. British authorities have reported carrying out sixty-nine searches of residences, businesses, vehicles, and open spaces, and have collected bomb-making equipment and chemicals, as well as more than 400 computers, 200 mobile telephones, 8,000 items of removable storage media such as memory sticks, CDs, and DVDs, some 6,000 gigabytes of data, and six "martyr videos." *See* Don Van Natta Jr. *et al.*, *In Tapes, Receipts and a Diary, Details of the British Terror Case*, N.Y. TIMES, Aug. 27, 2006, *available at* 2006 WLNR 16893012. CPS has filed charges against fifteen individuals in connection with its investigation. *See CPS Press Release: CPS Authorises Charges in Alleged Aircraft Terror Plot* (Aug. 21, 2006) *available at* http://www.cps.gov.uk/news/pressreleases; Alan Cowell, *Britain Charges 3 More Suspects With Plotting to Bomb Airplanes*, N.Y. TIMES, Aug. 30, 2006, *available at* 2006 WLNR 14995714. Offenses charged include conspiracy to murder pursuant to the U.K. Criminal Law Act 1997, "preparing acts of terrorism" pursuant to U.K.'s Terrorism Act 2006, "possession of articles useful to a person preparing an act of terrorism," and "failing to disclose information of material assistance in preventing an act of terrorism," both offenses under U.K.'s Terrorism Act 2000. Information from the searches conducted by British authorities will be reviewed in the coming months and disseminated for investigative purposes in support of these prosecutions.

U.S. prosecutors primarily receive U.K.-derived counterterrorism-related information through the FBI, with assistance from the FBI's

Legal Attaché office (Legat) in London. This informal process facilitates the flexible and rapid disclosure of information, and is acknowledged in the *United States Attorneys' Manual* (USAM) to be a proper channel for information sharing, although such informal means of obtaining foreign information may not yield evidence that would be admissible in a criminal trial. *See USAM*, Title 9; Criminal Resource Manual, 278.

RIPA provides safeguards to ensure that information disseminated from the United Kingdom is only used, disclosed, and distributed, to the least extent necessary for the purposes for which it was authorized. RIPA, § 15. To secure admissible evidence that conforms with the Federal Rules of Evidence, formal methods, although less flexible and oftentimes more time-consuming, may be required. The Office of International Affairs (OIA) assists prosecutors in choosing the proper means for obtaining admissible evidence from abroad through the use of letters rogatory, mutual legal assistance treaty (MLAT) requests, and executive agreements. Assistant U.S. Attorneys also must coordinate efforts to obtain international evidence in terrorism prosecutions with the Counterterrorism Section, as noted in the USAM. *See USAM,* Title 9-2.131 (Matters Assumed by Criminal Division or Higher Authority); Title 9-2.136 (Investigative and Prosecutive Policy for International Terrorism Matters); Title 9-2.155 (Sensitive Matters); and Title 9-2.400 (Prior Approvals Chart).

Successful terrorism prosecutions in the United States and the United Kingdom are frequently the result of close cooperation and the sharing of national security evidence within the law enforcement community. For example, in February 2006, Abu Hamza al Masri, a British militant Islamic preacher, was sentenced to seven years in prison, in the United Kingdom, for solicitation of murder and incitement of racial hatred. Hamza's arrest in the United Kingdom was based primarily upon evidence that was seized during a search of his residence at the time of his arrest on an extradition arrest warrant, which had been requested by the United States. Prosecutors in the United States and the United Kingdom (CPS) and investigators from the FBI and New Scotland Yard worked closely during the investigation. Currently, the United States is seeking Hamza's future extradition for charges based on his attempt to set up a jihad training camp in Oregon and his participation in a hostage-taking conspiracy, during which sixteen Western tourists were taken hostage in Yemen.

In another case, a jury convicted Ali Al-Timimi, a speaker and spiritual leader in Northern Virginia, on April 22, 2005, for encouraging and counseling others to go to Pakistan to receive military training from the foreign terrorist organization, Lashkar-e-Taiba, in order to fight against American troops. Both the British and Australian governments provided significant assistance in this and other related Northern Virginia prosecutions.

Other cooperation has come in the form of key witness testimony. For instance, British arms dealer, Hemant Lakhani, was convicted and sentenced in September 2005 to forty-seven years in prison, in the United States, for his role in attempting to sell an anti-aircraft missile to a man whom he believed represented a terrorist group intent on shooting down a United States commercial airliner. Witnesses from the United Kingdom and Russia testified in New Jersey federal court about the assistance they provided to their United States counterparts. Additionally, Mohammed Junaid Babar, a naturalized U.S. citizen, pled guilty to material support charges on June 3, 2004 in the United States. In the course of his cooperation with the FBI, he was the primary prosecution witness in a United Kingdom trial, in mid-2006, against seven suspects charged in the U.K. and Canada in connection with a U.K. bomb plot.

Recent close cooperation between U.S. and U.K. prosecutors has resulted in the United Kingdom's High Court ruling on November 30, 2006, which approved the extradition of two British citizens charged with terrorism offenses in the United States. The extraditions of Haroon Rashid Aswat, believed to have set up a terrorist training camp, and Babar Ahmed, wanted for conspiring to kill Americans and for running a Web site used to fund terrorists and recruit al Qaeda members, were conditioned upon U.S. assurances that the two would not be subject to the death penalty or a military commission.

Significant and ongoing cooperation between U.S. and U.K. law enforcement resulted in the conviction and forty-year sentence of Dhiren Barot that was imposed by a British court in November 2006, for conspiring to commit mass murder in the United States and the United Kingdom. In the course of his guilty plea, the

British court was provided details, by the United States, of Barot's involvement in plots to orchestrate potential attacks on significant institutions in both nations, including the International Monetary Fund and the New York Stock Exchange, as well as to detonate dirty bombs.

VII. Speech-based prosecution in the United Kingdom

Despite the significant evidentiary issues associated with using British-obtained evidence, recent amendments to the United Kingdom's terrorism laws provide British prosecutors with expanded charging options. Similar laws are unavailable to prosecutors in the United States because they contain provisions that could not be imported directly into American law consistent with the First Amendment. *See generally Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969) ("[T]he constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action."). For instance, under U.K. law, a person commits an offense if he incites another person to commit an act of terrorism wholly or partly outside the United Kingdom and the offense, if committed in the United Kingdom, would constitute any of several enumerated predicate offenses. Terrorism Act 2000, § 59.

Additionally, the ability to punish speech in favor of terrorism was expanded by the Terrorism Act 2006, and created new offenses for encouraging terrorism and disseminating terrorism publications. Under U.K. law, a statement that encourages terrorism and is likely to induce members of the public to commit or prepare terrorist acts may include a statement that "glorifies the commission or preparation" of such acts or offences. Terrorism Act 2006, § 1(1)-(3). Disseminating terrorism publications may include: distributing, circulating, giving, or selling a terrorist publication; transmitting the contents of such a publication electronically; providing a service that allows others to receive or view such publications; or possessing such a publication with a view to its becoming the subject of conduct described above. Terrorism Act 2006, § 2.

Under both provisions, the defendant must intend that his conduct induce the commission, preparation, or instigation of a terrorist act, intend to provide assistance in the commission or preparation of such acts, or he must be reckless with regard to either effect. Significantly, the prosecution need not prove that a terrorist act was committed under either section. *Id.* Of great interest internationally, the United Kingdom's Terrorism Act 2006 contains a section specifying the application of these encouragement and dissemination crimes to the Internet. Terrorism Act 2006, § 3.

VIII. Jurisdictional Memorandum of Understanding

In January 2007, the Attorneys General of the United States and the United Kingdom approved a document entitled "Guidance For Handling Criminal Cases With Concurrent Jurisdiction Between the United Kingdom and the United States of America" (hereinafter Guidance). Although not meant to replace existing mechanisms or lines of communication, this Guidance will assist investigators and prosecutors, in both countries, by providing an additional formal avenue for exchanging information in serious, sensitive, or complex criminal cases. These include counterespionage and counterterrorism cases, where it is apparent to prosecutors in one country that a prosecutor in the other country could, potentially, have an interest in prosecuting the case. ¶¶ 1-2. The goal of the Guidance is to provide a mechanism for establishing contact at the early stages of an investigation so that a coordinated decision can be made by both U.K. and U.S. prosecutors.

The Guidance provides that a U.S. prosecutor handling such a case should contact OIA, unless the case involves particularly sensitive or classified information, in which case the prosecutor should contact the office of the Assistant Attorney General for National Security in the National Security Division (NSD). ¶¶ 6, 9; Annex A. As noted earlier, terrorism-related cases require notification and ongoing consultation with the NSD, consistent with the requirements set out in the USAM. With the exception of cases in which a U.S. prosecutor already has an established contact in the United Kingdom, the OIA (or the NSD) will contact the appropriate prosecuting agency in the United Kingdom, or, alternatively, either the office of the Attorney General for England, Wales, and Northern Ireland or the office of the Lord Advocate of Scotland.

Similarly, the Guidance provides that whenever a U.K. prosecutor handling a serious, sensitive, or complex case becomes aware of issues arising from the possibility of concurrent jurisdiction with the United States, he should contact the appropriate person responsible in the United Kingdom to act as a liaison with OIA (or the NSD), as appropriate. ¶ 8.

The Guidance is meant to encourage discussions between U.S. and U.K. prosecutors to develop a case strategy, to share information about the facts of the case, key evidence, and any other information, in order to resolve issues of jurisdiction. Jurisdictional questions may include one or all of the following.

- Where and how the investigation may most effectively be prosecuted?
- Whether prosecutions should be initiated or discontinued?
- How aspects of the case could be more appropriately pursued in each jurisdiction?

¶¶ 11-13. Finally, the Guidance notes that it may be necessary for the offices of the Attorneys General or Lord Advocate to become involved to resolve issues of jurisdiction. ¶ 16.

IX. Conclusion

The global nature of terrorism necessitates early and extensive communication between international sovereigns, in order to determine the most effective means by which to prosecute terrorists who target the citizens of multiple countries. As noted above, the differences in the scope of U.K. and U.S. terrorism laws will often result in one course of action or jurisdiction of prosecution that will be most favorable to both countries. Only by working in concert and sharing critical information will the U.K. and the U.S. governments be able to develop an appropriate strategy in the early stages of a terrorism investigation, and continue to enjoy the types of success experienced in terrorism prosecutions to date. Such cooperation helped prevent the August 2006 aircraft plot from becoming a reality, and has led to the development of formal Guidance for law enforcement to forge stronger cooperation between the two nations.

The threat against U.S. and U.K. citizens, however, is far from over. Overwhelming amounts of evidence obtained internationally in the August 2006 plot will necessitate many months of forensic work, and trials are not expected to begin in the United Kingdom until 2008. In the meantime, and in the future, U.S. law enforcement must continue to work closely with their British counterparts to keep the channels of communication open and make sure that all leads are aggressively pursued in the best interests of both nations.❖

ABOUT THE AUTHOR

❑**Jocelyn A. Aqua** is a Trial Attorney with the Counterterrorism Section of the National Security Division. She joined the Department of Justice in 2002 and was an attorney in the Office of Intelligence Policy and Review until March 2006. Prior to joining the Department of Justice, Ms. Aqua was an associate at White and Case, LLP where her practice included complex international civil litigation and international arbitration. ✠

Request for Subscription Update

In an effort to provide the UNITED STATES ATTORNEYS' BULLETIN to all federal law enforcement personnel who wish to receive it, we are requesting that you e-mail Nancy Bowman (nancy.bowman@usdoj.gov) with the following information: Name, title, complete shipping address, telephone number, number of copies desired, and e-mail address. If there is more than one person in your office receiving the BULLETIN, we ask that you have one receiving contact and make distribution within your organization. If you do not have access to e-mail, please call 803-705-5659. Your cooperation is appreciated.