

NOTRE
DAME

After September 11:
Challenges, Choices



LAWYER

FALL/WINTER 2001

Combating Terrorism through Law Enforcement:

Crime-Fighting Adapts to the
New War on Terrorism



BY CATHY PIERONEK '84, '95 J.D.
DIRECTOR OF LAW SCHOOL RELATIONS

“Al-Qaida is to terror what the Mafia is to crime.”

President George W. Bush spoke these words in a speech to Congress a mere nine days after the terrorist attacks on September 11. Several weeks later, at an address to the summit meeting of the U.S. Conference of Mayors, U.S. Attorney General John Ashcroft declared that U.S. law enforcement would use the same tactics brought to bear against the mob in fighting the terrorists networks controlled by Osama bin Laden and shielded by the Taliban. But how apt is the analogy? And, more importantly, can the tactics used to combat the ordinary types of crimes committed by the mob — murder, drug trafficking, extortion — be used effectively against international terrorists?

Much of our popular image of efforts to fight organized crime comes from the movies. Shoot-outs in Chicago train stations. Raids on speakeasies. Smashing barrels of bootlegged liquor. All these exciting scenes, right from the movie *The Untouchables*, depict Hollywood’s version of the thrilling moments in fighting mob crime in the early part of the last century. And clearly, in the war against terrorism, there is a place for similarly aggressive military action, to physically disrupt the infrastructure of a country and the lives of those responsible for harboring terrorists.

But as everyone who has seen the movie knows, the federal government didn’t win its fight against the notorious Al Capone through these overt attempts to prevent or disrupt his criminal activity. The real hero of the story, as it turns out, was the accountant who found a way to prosecute the gangster for tax evasion, which kept him in prison for eight years.

Similarly, in our new war on terrorism, the federal government may find that its most effective weapons against Osama bin Laden and al-Qaida may lie in the same law-enforcement tools that have significantly disrupted organized criminal activity in recent years, according to Notre Dame Law School Professors G. Robert Blakey ’57, ’60 J.D., Jimmy Gurulé and Patricia Bellia.

But these tools must adapt to a new age of international electronic commerce and global communications, which add a tremendous level of complexity to an already daunting task. As one commentator has noted, if fighting the Mafia is likened to playing chess, fighting international terrorism may be likened to playing three-dimensional chess. In other words, it’s essentially the same game, but considerably more complex.

For much of the last century, efforts to fight mob-controlled criminal activity have depended on the creativity of federal law-enforcement officials. With tightly controlled networks of mob operatives, law enforcement faced tremendous difficulties in gathering the evidence necessary to prosecute gangsters for the crimes they committed. So, law enforcement had to use other, less direct, means to disrupt mob criminal activity.

In the early 1960s, the late U.S. Attorney General Robert F. Kennedy vowed to fight such criminal activity using whatever means he had at his disposal. According to current U.S. Attorney General John Ashcroft, speaking about those efforts before the U.S. Conference of Mayors summit meeting in Milwaukee, Wisconsin, on October 25, 2001, “Very often, prosecutors were aggressive, using obscure statutes to arrest and detain suspected mobsters. One racketeer and his father were indicted for lying on a federal home loan application. A former gunman for the Capone mob was brought to court on a violation of the Migratory Birds Act.” Although scores of murders and other heinous crimes remain unpunished, those involved were nevertheless prevented from engaging in such activities in the future through these aggressive law-enforcement tactics.





But legislation enacted in the latter part of the 20th century certainly helped to make law enforcement's job easier. In particular, racketeering (RICO) and money-laundering statutes added new weapons to the federal and state law-enforcement arsenal. Evidence-gathering improved as law-enforcement officials could listen in on the conversations of those planning or reminiscing about criminal activities. Criminal convictions could be secured with less prosecutorial creativity and more focus on actually illegal activities. Prosecutors and district attorneys can now go after individuals for being part of a criminal enterprise, even if direct evidence of any actual crime cannot be found. Criminal activity was further disrupted when the financial proceeds of those activities were confiscated and those responsible for moving the ill-gotten money through legitimate businesses were prosecuted for helping to finance and conceal the criminal enterprise.

And now, these statutes are being turned to another advantage — finding evidence against and disrupting the activities of the terrorists who turned our world upside down on September 11. But can laws written to curtail the mob also work against an international network of terrorists? Some commentators have suggested that, because the mob's motivation has

been primarily financial gain whereas the terrorists' motivation has been primarily power, that different tactics are needed. However, some Notre Dame Law School professors believe otherwise.

William and Dorothy O'Neill Professor of Law G. Robert Blakey '57, '60 J.D., who was instrumental in drafting the federal wiretapping and RICO statutes (along with the state-stature equivalents in more than half of the states that have adopted such legislation), has a clear picture of the usefulness of these laws. He believes that these statutes can be used to disrupt the activities of al-Qaida and Osama bin Laden in much the same way that they have been used to disrupt the activities of La Cosa Nostra and John Gotti.

As Professor Blakey explains, wiretapping had long been a part of the federal government's evidence-gathering arsenal. But in its 1967 ruling in a wiretapping case, *Katz v. United States*,¹ the U.S. Supreme Court expanded the understanding of the Fourth Amendment's protection against unreasonable searches and seizures by stating that the privacy right refers to the rights of the *person* being searched, not to the *place* where the search occurs. Consequently, wiretapping — of a public phone booth, in the case of *Katz* —

required authorization consistent with the safeguards required by the Fourth Amendment.

In the wake of this ruling, Congress enacted the federal wiretapping statute — Title III of the Crime Control Act of 1968 — to give federal courts the authority to issue wiretap orders in certain circumstances. This statute was amended in 1986 to include computer-based communications and to allow roving surveillance in certain narrow circumstances, when a suspect's actions have thwarted law-enforcement officials' surveillance efforts. So contrary to what has been reported in the popular media, according to Assistant Professor Patricia L. Bellia, the federal government has had the authority, for 15 years now, to intercept computer-based communications and to conduct roving wiretaps.

This is in contrast to laws governing access to certain information "about" communications — such as the phone number dialed, the e-mail address indicating the source or destination of a communication, or the address of an internet site visited. Although a 1986 statute provided clear rules for obtaining information about the phone number of an outgoing or incoming call — rules based on a Supreme Court decision indicating that a person does not have a privacy interest in such information



... because the changes brought about through the USA PATRIOT Act of 2001 mainly

bridge technical gaps in the existing statutory structure, Professor Bellia believes that the impact of these changes on privacy rights is far less dramatic than popular media accounts suggest.

— the statute did not explicitly provide similar rules for gathering similar computer-based information such as e-mail addresses or internet sites accessed. Nevertheless, Professor Bellia notes that law enforcement has operated under a general understanding that e-mail and other addresses in cyber-communications are analogous to phone numbers in telephone-based communications and, further, that law enforcement has consistently interpreted the statute to cover access to such addresses as well.

These statutes authorize surveillance in connection with criminal investigations of serious crimes, including terrorism-related offenses and offenses implicating national security. But these statutes exist alongside a separate statutory regime that deals exclusively with surveillance in national-security cases — that is, the Foreign Intelligence Surveillance Act of 1978 (FISA). FISA authorizes a special court to approve warrants for electronic surveillance to intercept telephone and cyber-based communications relevant to activities such as espionage, sabotage and terrorism. Again, however, the utility of this statutory scheme has been somewhat limited against the communications techniques employed by al-Qaida and other international terrorists, both because it

does not include roving wiretap authority analogous to the federal wiretapping statutes and because it requires that the government certify to the special court that the purpose of the surveillance is to obtain foreign intelligence information.

Legislation passed by Congress and signed by President Bush on October 26, 2001, will close some of these gaps in existing law, according to Professor Blakey. And because the changes brought about through the USA PATRIOT Act of 2001

mainly bridge technical gaps in the existing statutory structure, Professor Bellia believes that the impact of these changes on privacy rights is far less dramatic than popular media accounts suggest.

For example, the act codifies existing law-enforcement understanding about gathering certain non-private information from cyber-based communications such as e-mail addresses and addresses associated with other internet communications. In addition, the act provides for roving



What RICO requires, as Professor Blakey explains, is a predicate act — a crime — and an affiliation with the individual or individuals who committed the crime through the criminal enterprise.

wiretap authority under FISA that is analogous to the authority that had already existed under the federal wiretapping statutes.

Another provision in the act appears to expand law enforcement authority as well. According to Professor Bellia, however, this provision is merely a way to achieve with one court order what law enforcement could do already, but only with multiple court orders. Prior to the passage of the USA PATRIOT Act, tracking of non-content telephone and electronic communications information such as phone numbers called and e-mail and internet addresses accessed required law enforcement officials to obtain a new court order in each jurisdiction in which they sought information. The provisions of the new act, however, allow the government to serve one order on multiple service providers, thus giving a single order the broadest possible geographic scope.

One provision that popular media seems to have all but ignored, however, is what Professor Bellia describes as a subtle change to the language of FISA. She believes that this might well prove to be the most significant impact of the act, because it changes the requirements for issuing wiretapping orders related to foreign surveillance, and also because it might have Fourth Amendment implications in criminal prosecutions. According to Professor Blakey, under the original FISA, surveillance to gather information relevant to national security had to be the purpose of operating such a wiretap. If, through the FISA-authorized wiretap, the government *incidentally* came across information relating to criminal activities, the government could use that information in criminal prosecutions *only if* the government could prove that the wiretap was issued for the *primary* purpose of conducting national-security surveillance. The new provisions in the USA PATRIOT Act, however, allow the government to use such incidentally obtained information on a somewhat lesser showing that national security was a *significant* purpose of the wiretap. And as Professor Bellia notes, this raises concerns over whether FISA satisfies Fourth Amendment requirements, because it could broaden wiretap authority under

the statute beyond national-security surveillance and into criminal evidence-gathering.

In addition to these clarified and somewhat expanded evidence-gathering powers, the federal government may also prosecute those involved in aspects of the terrorist attacks beyond the actual execution of the aircraft hijackings and subsequent crashes. Under Title IX of the Omnibus Crime Control Act of 1970 — otherwise known as the Racketeer-Influenced Corrupt Organizations (RICO) statute, in the drafting of which Professor Blakey played a key role — the government may prosecute individuals involved in a criminal enterprise, even if those individuals did not actually commit a particular crime. What RICO requires, as Professor Blakey explains, is a predicate act — a crime — and an affiliation with the individual or individuals who committed the crime through the criminal enterprise. And to define this predicate act or crime — as perhaps distinct from the acts of war involved in destroying four U.S. aircraft and the World Trade Center, damaging the Pentagon and killing several thousand people on American soil — federal law enforcement has turned to the money-laundering statutes.

NDLS Professor Jimmy Gurulé, currently on leave to serve as undersecretary for the Office of Enforcement in the U.S. Treasury Department, firmly believes in the appropriateness of prosecuting terrorists — and other international criminals — using the Money Laundering Control Act of 1986 (MLCA), which was enacted originally to combat organized crime and drug trafficking. With certain enhancements to law enforcement powers granted through the Antiterrorism Act of 2001, Professor Gurulé, who is now the highest-ranking Latino law enforcement official in the country, believes that federal authorities now have the power they need to combat terrorism on a different front — that is, by putting a stop to the financial transactions that give terrorist groups the power to operate.

As he described in a 1995 article, Professor Gurulé characterizes money laundering “as the ‘lifeblood’ of international narcotics trafficking and traditional

And to define this predicate act or crime — as perhaps distinct from the acts of war involved in destroying four U.S. aircraft and the World Trade Center, damaging the Pentagon and killing several thousand people on American soil — federal law enforcement has turned to the money-laundering statutes.



Under Professor Gurulé's leadership, the Treasury Department has also initiated an effort called the Foreign Terrorist Asset Tracking (FTAT) Center, formed to tap into thousands of computer databases to track assets such as the money that funded the hijackers.

organized crime.”²² He notes that, in enacting the MLCA, “Congress was responding to the spiraling growth and pervasiveness of money laundering in the United States and the nexus between money laundering and organized crime.”²³ This nexus included not only the financial gains realized by organized crime and drug traffickers, but also the recycling of the ill-gotten money back into the enterprise to fund future criminal activity.

While the MCLA prohibits international money laundering, 18 U.S.C. § 1956(c)(7) limits the applicability of the statute to “specified unlawful activity,” which encompasses a wide range of statutorily designated felony offenses such as bank fraud, illegal gambling and narcotics trafficking. According to Professor Gurulé, what the Antiterrorism Act adds to this scheme is “authority for two additional

sanctions programs targeting terrorism.” In his testimony before the U.S. House of Representatives Committee on Financial Services, Professor Gurulé described those programs: “First, [the act] prohibit[s] material support, such as funds, false identifications and safe houses, to designated foreign terrorist organizations. Second, [it] prohibit[s] financial transactions with state sponsors of terrorism.”

Furthermore, in enforcing the provisions of the MLCA, the government must rely on suspicious-transaction reports provided by banks and other financial institutions. But as has been noted in the popular media lately, many of these terrorist-related financial transactions occur informally, outside the banking system. In the case of the terrorists, much of this money moves through a system of transfer networks called *hawalas*. According to

Professor Gurulé, the Bank Secrecy Act of 2001 will aid law-enforcement attempts to reach into this system by requiring these informal funds-transfer businesses to register with the Treasury Department by the end of 2001. In addition, the Treasury Department is working on similar suspicious-activity reporting rules relevant to casinos and to other nonbank financial institutions such as securities brokers and dealers.

Under Professor Gurulé's leadership, the Treasury Department has also initiated an effort called the Foreign Terrorist Asset Tracking (FTAT) Center, formed to tap into thousands of computer databases to track assets such as the money that funded the hijackers. In his recent House committee testimony, Professor Gurulé noted, “The complex nature of terrorist fund raising demands a creative and unconventional response from the U.S. government.” In exploring how key government officials have responded to the events of September 11, the October 29, 2001, edition of *NEWSWEEK* magazine notes that Professor Gurulé is addressing the problem in part by reevaluating how various government agencies can better share intelligence on such matters.

Through the work of FTAT, Professor Gurulé believes that the



government will be able to “identify the financial infrastructure of terrorist organizations worldwide and curtail their ability to move money through the international banking system.” In his congressional testimony, he commented that FTAT “represents a preventative, proactive and strategic approach to using financial data to target and curb terrorist funding worldwide.” In addition, three law enforcement agencies in the Treasury Department — the U.S. Customs Service, the Internal Revenue Service Criminal Investigations unit and the Secret Service, all of which fall under the Office of Enforcement — are working closely with the president’s Joint Terrorism Task Forces and at FBI headquarters to lend their technical expertise to tracking the terrorists’ money.

As Professor Gurulé explains, FTAT differs in two respects from traditional law-enforcement efforts to halt money laundering. First, traditional law-enforcement efforts focus on financial data in the context of a specific case. FTAT, however, looks at financial data across global terrorist organizations that have been implicated in a number of attacks.

Second, traditional law-enforcement efforts related to money laundering attempt to deter legitimate financial institutions from engaging in legal activities

that nevertheless abet the criminal conduct of organized crime or the narcotics-trafficking industry. Disrupting the operational ability of these criminals occurs not as the primary focus but, rather, as more of a by-product of these efforts. But through FTAT, as Professor Gurulé notes, federal law enforcement will collect and analyze information related to money laundering for the *express purpose* of identifying and disrupting the various sources of funding that these groups are receiving. In particular, FTAT will assess the sources and methods used by foreign terrorist groups to raise money and fund their activities. In Professor Gurulé’s words, “This information will [then] be used to conceptualize, coordinate and implement strategies within the U.S. government to achieve four goals: deny these target groups access to the international financial system; impair their fund-raising abilities; expose, isolate, and incapacitate their financial holdings; and to cooperate with other governments to take similar measures.”

Finally, Professor Gurulé and his colleagues in the Treasury Department are hard at work on efforts to secure international cooperation in these strategies to combat terrorism by attacking the financial structure of these organizations. The Office of Foreign Assets Control (OFAC),

which also reports to Professor Gurulé, administers economic sanctions programs against specific countries, groups or individuals that pose a threat to the national security, foreign policy or economy of the United States. OFAC has already played a key role in working with other countries to track terrorist money movements and will work with other nations to block terrorist assets, cut off the flow of money to the terrorists, and regulate more closely the fund-raising activities of a variety of organizations and groups.

“Al-Qaida is to terror what the Mafia is to crime.” But Jimmy Gurulé and others who continue to work on exploring ways to adapt existing legislation to fight the new war on terrorism are fast becoming to international terrorism what Eliot Ness, Robert F. Kennedy and G. Robert Blakey have been to organized crime: a formidable force dedicated to the destruction of those enterprises that wreak havoc on civilized society.

¹389 U.S. 347 (1967).

²Jimmy Gurulé, *The Money Laundering Control Act of 1986: Creating a New Federal Offense or Merely Affording Federal Prosecutors an Alternative Means of Punishing Specified Unlawful Activity?* 32 Am. Crim. L.Rev. 823, 823 (1995).

³*Id.* at 824.