U.S. Department of Justice

Office of Information and Privacy

Telephone: (202) 514-3642

Washington, D.C. 20530

JUL 17 2008

Kevin S. Bankston, Esq.
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

Re: DAG/05-R0327
OLP/05-R0329
OLA/05-R0330
CLM:LAD

Dear Mr. Bankston:

This is a final response to your Freedom of Information Act request dated January 13, 2005, and received in this Office on January 24, 2005, for records pertaining to "DOJ's understanding and use of its statutory authority to conduct Internet surveillance using so-called 'pen registers' and 'trap and trace devices,' both before and after the passage of the USA Patriot Act." This response is made on behalf of the Offices of the Deputy Attorney General, Legal Policy and Legislative Affairs. I apologize for the delay of this response, which was caused by the need to consult with other Department components.

We have completed our searches in the Offices of the Deputy Attorney General, Legal Policy and Legislative Affairs and have located twenty-six documents, totaling two-hundred and eighty-five pages that are responsive to your request. I have determined that seventeen documents, totaling one-hundred and ninty-three pages are appropriate for release without excision and copies are enclosed. Please be advised that portions of these documents contained information that was outside of the scope of your request. We have redacted such information and marked it accordingly. Additionally, two documents, totaling five pages are appropriate for release with excisions made pursuant to Exemptions 5 and 6 of the FOIA, 5 U.S.C. § 552(b)(5), (6). Three documents, totaling twenty-three pages are being withheld in full at the request of the Criminal Division pursuant to Exemption of the FOIA, 5 U.S.C. § 552(b)(5).

Exemption 5 pertains to certain inter- and intra-agency communications protected by the deliberative process privilege. Exemption 6 pertains to information the release of which would constitute a clearly unwarranted invasion of the personal privacy of third parties. For your information, the withheld material consists of deliberative memoranda, e-mail, and personal telephone numbers. Finally, please be advised that we referred one document, totaling ten pages to the Federal Bureau of Investigation and six documents, totaling one-hundred and forty-four pages to the Criminal Division for processing and direct response to you. Please be advised that four additional responsive documents consisting of congressional testimony by former Attorney General Alberto Gonzales, Deputy Attorney General James Comey and Assistant Attorney General Viet Dinh were located and are publicly available on the Senate and House Judiciary Committees' website.

If you are not satisfied with my response, you may administratively appeal by writing to the Director, Office of Information and Privacy, United States Department of Justice, Suite 11050, 1425 New York Avenue, NW, Washington, D.C. 20530-0001, within sixty days from the date of this letter. Both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal."

Sincerely,

Carmen L. Mallon
Chief of Staff

U.S. Department of Justice

Office of the Deputy Attorney General

The Deputy Attorney General

Washington, D.C. 20530

May 24, 2002

MEMORANDUM

TO: THE ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION
THE ASSISTANT ATTORNEY GENERAL, ANTITRUST DIVISION
THE ASSISTANT ATTORNEY GENERAL, TAX DIVISION
ALL UNITED STATES ATTORNEYS
THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
THE ADMINISTRATOR OF THE DRUG ENFORCEMENT ADMINISTRATION
THE COMMISSIONER OF THE IMMIGRATION AND NATURALIZATION SERVICE
THE DIRECTOR OF THE UNITED STATES MARSHALS SERVICE

FROM: Larry D. Thompson

SUBJECT: Avoiding Collection and Investigative Use of "Content" in the Operation of Pen Registers and Trap and Trace Devices

This Memorandum sets forth the Department's policy regarding avoidance of "overcollection" in the use of pen registers and trap and trace devices that are deployed under the authority of chapter 206 of Title 18, United States Code, 18 U.S.C. § 3121, *et seq.*[1]

The privacy that Americans enjoy in the content of their communications – whether by telephone, by facsimile, or by email – is a basic and cherished right. Both the Fourth Amendment and federal statutory law provide important protections that collectively help to ensure that the content of a person's private communications may be obtained by law enforcement only under certain circumstances and only with the proper legal authorization. In updating and revising the statutory law in this area, the recently enacted USA Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) ("the Act"), draws the appropriate balance between the right of individuals to maintain the privacy of their communications and the need for law enforcement to obtain the evidence necessary to prevent and prosecute serious crime.

[1] The authorities granted by the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801, *et seq.*, are outside the scope of this Memorandum.

3

In particular, Section 216 of the Act revised and clarified existing law governing "pen registers" and "trap and trace" devices – which record limited information concerning the "processing and transmitting" of communications (such as the telephone numbers dialed on a phone) – so that these devices may clearly be used, not just on telephones, but in the context of any number of communications technologies.

At the same time, several provisions of the Act underscore the importance of avoiding unauthorized collection or use, by government agents, of the *content* of wire or electronic communications. In order to accomplish this important goal, this Memorandum briefly describes the relevant law and the changes made by the Act, and then sets forth Departmental policies in this area. Those policies include the following:

- Reasonably available technology must be used to avoid collection of any content.
- If, despite use of reasonably available technology, some collection of a portion of content occurs, *no* affirmative investigative use may be made of that content.
- Any questions about what constitutes "content" must be coordinated with Main Justice.

Prior Law Governing Pen Registers and Trap and Trace Devices. Since 1986, the use of "pen registers" and "trap and trace" devices has been governed by the provisions of chapter 206 of Title 18, United States Code. *See* 18 U.S.C. § 3121, *et seq*. Prior to the recent enactment of the USA Patriot Act, a "pen register" was defined in chapter 206 as "a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached." 18 U.S.C. § 3127(3). Analogously, a "trap and trace" device was defined as "a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted." *Id*., § 3127(4). Thus, a pen register could be used to record the numbers of all outgoing calls on a telephone, and a trap and trace device could be used to record the numbers of all incoming calls.

Because the Supreme Court has held that this sort of limited information concerning the source and destination of a communication is not protected by the Fourth Amendment's warrant requirement, *see Smith v. Maryland*, 442 U.S. 735 (1979), chapter 206 permitted an order authorizing a pen register or trap and trace device to be issued without showing probable cause. Instead, an order shall be issued if the Government "certifie[s] that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." 18 U.S.C. § 3123(a) (2000). By contrast, the *contents* of a telephone conversation are generally protected by the Fourth Amendment, *see Katz v. United States*, 389 U.S. 347 (1967), as well as by the more extensive procedural protections of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 212 (1968), *codified as amended at* 18 U.S.C. § 2510, *et seq*. ("Title III").

In enacting the provisions of Chapter 206 governing pen registers and trap and trace devices, Congress also amended Title III to exempt pen registers and trap and trace devices from the requirements of the latter statute. *See* Pub. L. 99-508, § 101(b), 100 Stat. 1848 (1986) (adding 18 U.S.C. § 2511(h)(i)). However, in order to address the possibility that a pen register might, due to technological limitations, obtain some limited measure of "content," Congress later specifically provided in chapter 206 that an agency authorized to use a pen register must "use technology reasonably available to it" that restricts the information obtained to that used in "call processing." Pub. L. No. 103-414, § 207(b), 108 Stat. 4279 (1994) (amending 18 U.S.C. § 3121(c)).

Relevant Amendments made by the USA Patriot Act. The Act made several changes to chapter 206 that are of relevance here. In particular, section 3121(c) was amended to make explicit what was already implicit in the prior provision, namely, that an agency deploying a pen register must use "technology reasonably available to it" that restricts the information obtained "so as not to include the contents of any wire or electronic communications." The amended section 3121(c) now reads, in full, as follows:

> A governmental agency authorized to install and use a pen register or trap and trace device under this chapter or under State law *shall use technology reasonably available to it* that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications *so as not to include the contents of any wire or electronic communications.*

18 U.S.C. § 3121(c), as amended by Pub. L. No. 107-56, § 216(a), 115 Stat. at 288 (emphasis added).

Similarly, in amending the definitions of "pen register" and "trap and trace device" to make them more technologically neutral, the Act again expressly reiterates what was already implicit in the prior statute, namely, that a pen register or a trap and trace device is not to be viewed as an affirmative authorization for the interception of the content of communications. Thus, the amended definition of a "pen register" now provides, in pertinent part:

> [T]he term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, *provided, however, that such information shall not include the contents of any communication*
> . . . .

18 U.S.C. § 3127(3), as amended by Pub. L. No. 107-56, § 216(c)(2), 115 Stat. at 290 (emphasis added). Likewise, the Act amends the definition of "trap and trace device" so that it now provides:

> [T]he term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, *provided, however, that such information shall not include the contents of any communication* . . . .

18 U.S.C. § 3127(4), as amended by Pub. L. No. 107-56, § 216(c)(3), 115 Stat. at 290 (emphasis added).

Department Policy Regarding Avoidance of "Overcollection" in the Use of Pen Registers and Trap and Trace Devices. Although, as noted, the Act's specific addition of references to "content" in chapter 206 probably does not alter pre-existing law on this point, it is appropriate, in light of Congress' action, to clearly delineate Department policy regarding the avoidance of "overcollection," *i.e.*, the collection of "content" in the use of pen registers or trap and trace devices under chapter 206. This policy includes the following basic principles.

1. **Use of reasonably available technology to avoid overcollection.** As mandated by section 3121(c), an agency seeking to deploy a pen register or trap and trace device must ensure that it uses "technology reasonably available to it" that restricts the information obtained "so as not to include the contents of any wire or electronic communications." 18 U.S.C. § 3121(c) (West Supp. 2002). This provision imposes an affirmative obligation to operate a pen register or trap and trace device in a manner that, to the extent feasible with reasonably available technology, will minimize any possible overcollection while still allowing the device to collect all of the limited information authorized.

Moreover, as a general matter, those responsible for the design, development, or acquisition of pen registers and trap and trace devices should ensure that the devices developed or acquired for use by the Department reflect reasonably available technology that restricts the information obtained "so as not to include the contents of any wire or electronic communications."

2. **No affirmative investigative use of any overcollection that occurs despite use of reasonably available technology.** To the extent that, despite the use of "technology reasonably available to it," an agency's deployment of a pen register does result in the incidental collection of some portion of "content," it is the policy of this Department that such "content" may not be used for any affirmative investigative purpose, except in a rare case in order to prevent an immediate danger of death, serious physical injury, or harm to the national security. For example, if, despite the use of reasonably available technology, a telephone pen register incidentally recorded a bank account number and personal identification number (PIN) entered on an automated bank-by-phone system, those numbers should not be affirmatively used for any investigative purpose.

Accordingly, each agency must take steps to ensure that any incidental collection of a portion

of "content" is not used for any affirmative investigative purpose.[2] Investigating agencies should take appropriate measures to ensure compliance with this directive, and United States Attorneys should likewise ensure that federal prosecutors do not make any investigative use of such content, whether in court applications or otherwise.

3. **Coordination of issues concerning what constitutes "content"**. In applying the above principles, agencies should be guided by the definition of "content" that is contained in Title III: the term "content" is there defined to include "any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8) (West Supp. 2002). Similarly, in describing the sort of information that pen registers and trap and trace devices are designed to capture, the provisions of Chapter 206 make clear that "dialing, routing, addressing or signaling information" that is used in "the processing and transmitting of wire or electronic communications" does not, without more, constitute "content." 18 U.S.C. § 3127(3) (West Supp. 2002); *id.*, § 3121(c).

The Assistant Attorney General for the Criminal Division (AAG) should ensure that the Criminal Division provides appropriate guidance, through amendments to the United States Attorneys' Manual or otherwise, with respect to any significant general issues concerning what constitutes the "content" of a communication.

To the extent that, in applying the above principles, specific issues arise over whether particular types of information constitute "content," such questions should be addressed, as appropriate, to the Office of Enforcement Operations in the telephone context (202-514-6809) or the Computer Crime and Intellectual Property Section in the computer context (202-514-1026).

Construction of this Memorandum. This Memorandum is limited to improving the internal management of the Department and is not intended to, nor does it, create any right, benefit, or privilege, substantive or procedural, enforceable at law or equity, by any party against the United States, the Department of Justice, their officers or employees, or any other person or entity. Nor should this Memorandum be construed to create any right to judicial review involving the compliance or noncompliance of the United States, the Department, their officers or employees, or any other person or entity, with this Memorandum.

---

[2] This is not to say that an agency should not retain a file copy of all of the information it received from a pen register or trap and trace device. An agency may be statutorily *required* to keep a record of all of the information it obtains with a particular pen register or trap and trace device, *see, e.g.*, 18 U.S.C. § 3123(a)(3), *as amended by* Pub. L. No. 107-56, § 216(b)(1), 115 Stat. at 289 (requiring that, in certain limited circumstances, an agency must maintain and file with the issuing court a record of "any information which has been collected by the device"), and, in the event of a subsequent prosecution, the agency may be required to produce to defense counsel a complete record of what was recorded or captured by a pen register or trap and trace device deployed by the agency in a particular case. This Memorandum prohibits *affirmative investigative* uses. Accordingly, nothing in this Memorandum should be construed to preclude an agency from maintaining a record of the full information obtained by the agency from a pen register or trap and trace device.

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

August 26, 2002

The Honorable F. James Sensenbrenner, Jr.
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

Enclosed please find responses to questions posed to the Attorney General on USA PATRIOT Act implementation in your letter of June 13, 2002, co-signed by Ranking Member Conyers. An identical response will be sent to Congressman Conyers.

We appreciate the additional time provided to the Department to submit responses to your questions. On July 26, 2002, the Department provided answers to 28 out of the 50 questions. With this letter, we are pleased to forward to the Committee the remaining questions.

The Department remains committed to working with the Committee as we continue to implement these important new tools for law enforcement in the fight against terrorism. If we can be of further assistance on this, or any other matter, please do not hesitate to contact this office.

Sincerely,

Daniel J. Bryant
Assistant Attorney General

Enclosure

Questions Submitted by the House Judiciary Committee
to the Attorney General on USA PATRIOT Act Implementation

Submission 2 of 2

2.

OUT OF SCOPE

[redacted]

[redacted]

6.

[redacted]

[redacted]

7.

[redacted]

[redacted]

OUT OF SCOPE

[redacted]

13. **How many roving pen register and trap and trace orders have been issued under section 216 of the Act?**

Answer: None. Section 216 of the act did not create the authority for a "roving" pen register or trap and trace device, as that term is commonly understood in the context of a court order for the interception of the content of communications. Unlike a "roving" wiretap order, a pen/trap order does not follow the target from one "telephone" to another. Instead, the order identifies the facility at which the pen/trap device will be installed, and it allows the government to uncover the true source or destination of communications to or from that facility even if several different companies in different judicial districts carry those communications. Accordingly, no roving pen register and trap and trace orders have been issued under section 216 of the Act.

Section 216 does authorize a court to order "the installation and use of a pen register or trap and trace device anywhere within the United States." Although the exact number of pen/trap orders that have been executed outside of the district of the authorizing magistrate is unknown, such orders have proved to be critically important in a variety of terrorist and criminal investigations. In particular, out-of-district orders have been used to trace the communications of (1) terrorist conspirators, (2) kidnappers who communicated their demands via e-mail, (3) a major drug distributor, (4) identity thieves who obtained victims' bank account information and stole their money, (5) a fugitive who fled on the eve of trial using a fake passport, and (6) a four-time murderer.

How many "Armey" notices, reporting on the details of the installation of roving pen registers or trap and trace devices, have been filed with U.S. courts pursuant section 216 of the Act?

Answer: We are aware of two instances where 18 U.S.C. § 3123(a)(3), as amended by section 216 of the Act (the "Armey Amendment"), required the filing of notices pertaining to a pen/trap order executed by the Federal Bureau of Investigation. That provision requires the filing of records within 30 days after termination of the order (including any extensions thereof).

How many "Armey" notices were related to a terrorism investigation?

Answer: One (1) of the two (2) instances referenced above. OUT OF SCOPE

16. [redacted]

18. [redacted]

20. [redacted]

Pages 4-21 are outside the scope of the request

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

August 26, 2002

The Honorable John Conyers, Jr.
Ranking Minority Member
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

Dear Congressman Conyers:

Enclosed please find responses to questions posed to the Attorney General on USA PATRIOT Act implementation in your letter of June 13, 2002, co-signed by Chairman F. James Sensenbrenner, Jr. An identical response will be sent to Chairman Sensenbrenner.

We appreciate the additional time provided to the Department to submit responses to your questions. On July 26, 2002, the Department provided answers to 28 out of the 50 questions. With this letter, we are pleased to forward to the Committee the remaining questions.

The Department remains committed to working with the Committee as we continue to implement these important new tools for law enforcement in the fight against terrorism. If we can be of further assistance on this, or any other matter, please do not hesitate to contact this office.

Sincerely,

Daniel J. Bryant
Assistant Attorney General

Enclosure

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

August 26, 2002

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Pursuant to your request of the Attorney General at the Committee's July 25, 2002 oversight hearing of the Department of Justice, we are enclosing the Department's second set of answers to questions submitted by the House Judiciary Committee on USA PATRIOT Act implementation, in their June 13, 2002 letter.

On July 26, 2002, the Department provided answers to 28 out of the 50 questions to the House Committee on the Judiciary. With this letter, we are pleased to forward to you the remaining questions which have been transmitted to the Committee.

The Department is continuing to address the questions posed in the July 24, 2002 letter from Senator Feingold, in his capacity as Constitution Subcommittee Chairman. If we can be of further assistance on this, or any other matter, please do not hesitate to contact this office.

Sincerely,

Daniel J. Bryant
Assistant Attorney General

cc: The Honorable Orrin G. Hatch
Ranking Member

Enclosure

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

August 26, 2002

The Honorable Russell D. Feingold
Chairman
Subcommittee on the Constitution
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

In response to your July 24, 2002 letter to the Attorney General, we are enclosing the Department's second set of answers to questions submitted by the House Judiciary Committee on USA PATRIOT Act implementation, in their June 13, 2002 letter.

On July 26, 2002, the Department provided answers to 28 out of the 50 questions to the House Committee on the Judiciary. With this letter, we are pleased to forward to you the remaining questions which have been transmitted to the Committee.

The Department is continuing to address the remaining questions posed in your letter and will forward them to you as soon as possible. If we can be of further assistance on this, or any other matter, please do not hesitate to contact this office.

Sincerely,

Daniel J. Bryant
Assistant Attorney General

Enclosure

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

September 20, 2002

The Honorable F. James Sensenbrenner, Jr.
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

On July 26 and August 26, the Department submitted written responses to questions posed by the Committee in your letter of June 13, 2002 on USA PATRIOT Act implementation, co-signed by Congressman John Conyers. The Department was subsequently contacted by staff of the Judiciary Committee seeking additional information on a number of the responses. Enclosed please find responses to those follow-up questions.

Additionally, part of the answer to follow-up question number 11 requires the submission of classified information. As such, the information will be provided to the Committee under separate cover.

Thank you for this opportunity to provide additional information to the Committee on implementation of the USA PATRIOT Act. If we can be of further assistance on this, or any other matter, please do not hesitate to contact this office.

Sincerely,

Daniel J. Bryant
Assistant Attorney General

Enclosure

cc: The Honorable John Conyers, Jr.
Ranking Minority Member

Page 1 is outside the scope of the request

OUT OF SCOPE

[redacted]

10. **Follow-up Question: Can the practices referred to ensure that pen\traps are not made solely for 1st Amendment activities be made public or otherwise provided to the Committee?**

Answer: A great deal of care is given to ensure that an order authorizing the installation and use of a pen register or trap and trace device is not sought solely on the basis of activities protected by the First Amendment. In each case in which an order is sought from the Foreign Intelligence Surveillance Court, the attorney for the government conducts a review of the factual basis underlying the investigation and the request for pen/trap authority. The Attorney General or his designee, the Counsel for Intelligence Policy (the head of Office of Intelligence Policy and Review), personally approves the filing of every application with the Court. A brief statement of facts in each case is then presented to the Court, along with the Government's certification, signed by the individual applicant, that the order is not being sought solely for activities protected by the First Amendment.

11. [redacted]

OUT OF SCOPE

[redacted]

Pages 3-6 are outside the scope of the request

Congressional Statement
Federal Bureau of Investigation

October 9, 2002

Statement for the Record of
Dennis Lormel
Chief, Terrorist Financing Operations Section, Counterterrorism Division
Federal Bureau of Investigation

on
USA PATRIOT ACT/Terrorism Financing Operations Section

Before the
Senate Judiciary Committee
Subcommittee on Technology, Terrorism, and Government Information

Introduction

Good morning, Madam Chairman, and members of the Subcommittee on Technology, Terrorism, and Government Information. On behalf of the Federal Bureau of Investigation (FBI), I would like to express my gratitude to the Subcommittee for affording us the opportunity to participate in this forum and to update the Subcommittee on our use of the tools established within the framework of the USA PATRIOT Act and the work being conducted by our Terrorism Financing Operations Section.

As this Subcommittee is well aware, the FBI, in conjunction with law enforcement and intelligence agencies throughout the United States and the world, is engaged in the largest, most complex and perhaps the most critical criminal and terrorism investigation in our history. The FBI continues to dedicate considerable resources to this investigation and remains committed to determining the full scope of these terrorist acts, identifying all those involved in planning, executing and/or assisting in any manner the commission of these acts and others, and bringing those responsible to justice. The FBI will continue to exercise its leadership role in the global war on terrorism by taking all possible steps to prevent any further acts of terrorism.

The war on terrorism will be a long-term battle. It will not be won overnight nor will it be won without the highest levels of cooperation and coordination among law enforcement and intelligence agencies around the globe. Terrorism knows no borders or boundaries. The threat is not limited to any one region of the world. Law enforcement and intelligence agencies throughout the world possess tremendous resources and expertise. Allying these resources against the common enemy of terrorism is the key to dismantling these organizations and eliminating the threat they pose. Make no mistake about it, even with the combined resources and expertise possessed by law enforcement, the threat posed by terrorism is grave. Terrorists do not play by the rules of a civilized society, nor do they respect human decency. They will stop at nothing to commit acts of terror.

From a law enforcement perspective, success in the war on terrorism must be measured in our ability to prevent future acts of terrorism. Whether it be through prosecution, disruption, blocking/freezing of funds, or allowing a funding mechanism to remain in place in order to further an investigation, prevention remains the overarching focus. In this regard, fighting the war on terrorism requires powerful tools. The FBI appreciates the tools provided by the Congress in enacting the USA Patriot Act, including those contained within Title III of this Act, which is also know as the International Money Laundering Anti-Terrorist Financing Act of 2001.

The Terrorist Financing Operations Section (TFOS)

I would like to start my discussion regarding the FBI's use of the USA Patriot by focusing on the tools provided within Title III. To illustrate how these anti-money

7

laundering provisions aid our investigative efforts, it is necessary to understand how the FBI has been restructured to address terrorist financing matters. Identifying and tracking the financial structure supporting terrorist groups is critical to dismantling the organization and preventing future attacks. As in ordinary criminal investigations, "following the money" identifies, links, and develops evidence against those involved in criminal activity. In the early stages of the investigation into the events of September 11, 2001, it was financial evidence that quickly established links between the hijackers and identified co-conspirators.

It was also in the early stages of this investigation that the FBI and Department of Justice (DOJ) identified a critical need for a more comprehensive, centralized approach to terrorist financial matters. In response, the FBI established an interagency Terrorism Financial Review Group (TFRG), operating out of FBI Headquarters. By bringing together vast databases and the expertise of numerous federal agencies, the TFRG, which was subsequently expanded, renamed the Terrorist Financing Operations Section (TFOS), and assigned to the FBI's Counterterrorism Division, focuses a powerful array of resources on the financial tentacles of terrorist organizations.

The TFRG was created with a two-fold mission. First, it was designed to conduct a comprehensive financial analysis of the 19 hijackers to link them together and to identify their financial support structure within the United States and abroad. Through the execution of this mission, the TFRG was able to establish how the hijackers responsible for the attacks received their money, details of their flight training, where they lived, and details concerning individuals associated with the hijackers. The 19 hijackers opened 24 domestic bank accounts at four different banks. The TFOS analyzed the data associated with these accounts to develop a financial profile that has been used in connection with the FBI's investigation regarding the events of September 11, 2001.

The second aspect of the TFRG's mission was to serve as a template for preventive and predictive terrorist financial investigations. This mission, consistent with the TFRG's restructuring into the TFOS, has since evolved into a broader effort to identify, investigate, prosecute, disrupt, and dismantle all terrorist-related financial and fundraising activities.

To accomplish this mission, the TFOS has implemented initiatives to address all aspects of terrorist financing. For example, the TFOS is engaged in an aggressive international outreach program to share information regarding terrorist financing methods with the financial community and law enforcement, and has built upon long-established relationships with the financial services community in the United States and abroad. The international outreach initiative is coordinated through the network of FBI Legal Attache Offices located in 44 key cities worldwide, providing coverage for more than 200 countries and territories.

As touched upon earlier, a significant focus of the TFOS' efforts is prediction and prevention. In this regard, it has developed numerous data mining projects to provide further predictive abilities and maximize the use of both public and private database information. These efforts are complemented by the centralized terrorist financial database which the TFOS developed in connection with its coordination of financial investigation of individuals and groups who are suspects of FBI terrorism investigations. The TFOS has cataloged and reviewed financial documents obtained as a result of numerous financial subpoenas pertaining to individuals and accounts. These documents have been verified as being of investigatory interest and have been entered into the terrorist financial database for linkage analysis. The TFOS has obtained financial information from FBI Field Divisions and Legal Attache Offices, and has reviewed and documented financial transactions. These records include foreign bank accounts and foreign wire transfers. The information contained within the aforementioned database is being used to identify terrorist cells operating in the United States and abroad to prevent further terrorist acts. The TFOS meets regularly with representatives from the banking community and the financial services industry to share information and to refine methods to detect and identify potential terrorists around the world.

The TFOS created and continues to update a financial control list which contains names and identifying data for individuals under investigation for potential links to terrorist organizations. These lists are regularly shared with domestic and international law enforcement and intelligence agencies, and with the Federal Reserve Board, which disseminates the lists to financial institutions so they can flag