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

suspicious financial activity.

The TFOS regularly shares information with Customs' Operation Green Quest and provides daily downloads from its database to Green Quest and the Financial Crimes Enforcement Network (FinCEN). Further, the TFOS is working with FinCEN to explore new ways to data mine the Suspicious Activity Report (SAR), Currency Transaction Report (CTR), and Currency and Monetary Instrument Report databases.

Based on its international investigative abilities, and its close association with the Intelligence Community, the TFOS is in a unique position to coordinate anti-terrorism financial investigations and to ensure those investigations are coordinated with the goals and objectives of the FBI's Counterterrorism Program.

Use of the USA PATRIOT Act

I would now like to discuss how the TFOS has been making use of the tools established by the USA PATRIOT Act. Terrorist financing methods range from the highly sophisticated to the most basic. Traditionally, their efforts have been aided considerably by the use of correspondent bank accounts, private banking accounts, offshore shell banks, bulk cash smuggling, identity theft, credit card fraud, and other criminal operations. Informal Value Transfer Systems, such as "Hawalas," also present problems for law enforcement. They permit terrorists a means of transferring funds that is difficult to detect and trace. These informal systems are commonplace and appear to serve as an efficient means of transacting in mostly "cash" societies such as Pakistan, Afghanistan, and the Phillippines. In applying provisions of the USA PATRIOT Act we seek to erode the effectiveness of such methods without unduly undermining the legitimate economic activity that may rely on them. The Act establishes stricter rules for correspondent bank accounts, requires securities brokers and dealers to file SARs, and certain cash businesses to register with FinCEN and file SARs for a wider range of financial transactions.

The Act contains many other provisions that the FBI believes will considerably aid our efforts to address terrorist financing. These include the authority to seize terrorist assets, and the addition of terrorism and other offenses to the list of racketeering offenses. The utilization of this aspect of the USA PATRIOT Act is perhaps best exemplified through actions that have been taken against Non-Governmental Organizations (NGOs) believed to provide financial support to know Foreign Terrorist Organizations and other affiliated Terrorist Cells. As in the case of Halawas, the funding of terrorist organizations such as Al Qaeda and Hamas through NGOs and charitable organizations represents a significant challenge to law enforcement. Funding of terrorism through NGOs is a prime focus of terrorist financial investigations. NGOs may be large international organizations which can be exploited by individual employees sympathetic to terrorist causes through local branch offices; they may be private NGOs which exist solely to support a militant cause; or they may be closely affiliated with a state sponsor of terrorism. One of the challenges in investigations involving terrorist fundraising through NGOs is distinguishing terrorist fundraising activities from legitimate or what may appear to be legitimate charitable fundraising. Fundraising on the part of terrorist groups which on the surface appear to be efforts to "help the poor" or fundraising for charitable, humanitarian or other legitimate purposes actually falls squarely in the realm of logistical support for terrorist activity.

As a participant on the National Security Council's Policy Coordinating Committee (PCC) on terrorist finance, the TFOS participates in the effort to target NGOs believed to provide financial support to known Foreign Terrorist Organizations and affiliated terrorist cells. The PCC coordinates the development and implementation of policies to combat terrorist financing and provides analysis on these issues. Numerous FBI Field Offices have open investigations into organizations that may be funneling money to Foreign Terrorist Organizations and the TFOS has acted as a clearinghouse for these cases and has summarized the collected data.

In order to disrupt terrorist financing channels, the TFOS has coordinated FBI terrorist investigations with the terrorist designation and asset freezing efforts of the OFAC and Operation Green Quest. These efforts have resulted in the freezing of millions of dollars in foreign and US bank accounts. Specifically, the joint efforts targeting Al-Barakaat, the Holy Land Foundation for Relief and Development, the Global Relief Foundation, and the Benevolence International Foundation have resulted in the execution of numerous search warrants and the disruption of the fundraising and money remittance operations of these and other organizations. Financial

investigations of these entities have revealed that approximately $200 million in contributions passed through these organizations each year.

The USA PATRIOT Act also enables prosecutors to seize money subject to forfeiture in a foreign bank account by authorizing the seizure of a foreign bank's funds held in a U.S. correspondent account. Other important provisions expand the ability to prosecute unlicensed money transmitters, allow law enforcement faster access to reports of currency transactions in excess of $10,000, and provide authority for the service of administrative subpoenas on foreign banks concerning records of foreign transactions. This latter provision allows law enforcement to obtain critical information in an investigation on a more timely basis than was possible before. In counterterrorism investigations, of course, speed is of the essence because prevention is the goal.

Section 362 of the USA PATRIOT Act mandates that FinCEN establish a highly secure network to 1) allow financial institutions to file SARs and CTRs on-line, and 2) "provide financial institutions with alerts and other information regarding suspicious activities that warrant immediate and enhanced scrutiny." FinCEN has developed the USA Patriot Act Communication System to meet this mandate and is implementing the system. This will be a valuable tool for law enforcement, but it will require the full cooperation of private financial institutions. The TFOS has worked with financial institutions, and has provided to them information to help detect patterns of activity possibly associated with terrorist activity and the PACS will help considerably in these efforts.

Use of Other Provisions of the USA PATRIOT Act

In addition to the provisions effecting changes to money laundering statutes, the USA PATRIOT Act effected changes in national security authorities, the substantive criminal law, immigration law, and victim assistance statutes, and other areas. In particular, the Act seeks to improve the efficiency of the process associated with the FBI's conduct of electronic surveillance and physical searches authorized through the Foreign Intelligence Surveillance Act (FISA) of 1978 and to remove barriers to the timely sharing of information between counterintelligence and counterterrorism intelligence operations and criminal investigations. These enhancements in efficiency improve our ability to detect and prosecute offenders, and with less disruption to legitimate commerce. I would now like to highlight those provisions that the FBI has been utilizing most often in connection with the execution of its counterterrorism responsibilities.

Changes in Predicate Standards for National Security Letters (NSLs)

NSLs are administrative subpoenas that are issued in counterintelligence and counterterrorism investigations to obtain telephone and electronic communications records from telephone companies and Internet Service Providers (pursuant to the Electronic Communications Privacy Act, or ECPA); records from financial institutions (pursuant to the Right to Financial Privacy Act); and information from credit bureaus (pursuant to the Fair Credit Reporting Act). Delay in obtaining NSLs has long been identified as a significant problem relative to the conduct of counterintelligence and counterterrorism investigations. Two factors contributed most prominently to this delay. These were the complexity of the standard predication for NSLs and the requirement that signature authority be restricted to officials no lower than a Deputy Assistant Director at FBI Headquarters.

Section 505 of the USA Patriot changed the standard predication for all three types of NSLs to one requiring that the information being sought through the NSL is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States." Prior to the Act, the statutes required both relevance and "specific and articulable facts" giving reason to believe that the subject is an agent of a foreign power, or, in the case of subscriber requests, had been in contact with such an agent. This "agent of a foreign power" prong of the standard made it necessary to collect and document specific facts demonstrating that the standard had been met. This requirement and the complexity of the standard itself often led to extensive delays in generating NSLs.

Section 505 also allowed the Director to delegate signature authority for NSLs to

Special Agents in Charge serving in designated field divisions. The provisions delineated within Section 505 have resulted in investigators receiving the data needed in the furtherance of ongoing investigations in a more timely fashion, which in turn has had a positive impact on numerous investigations.

"Roving" FISA Electronic Surveillance Authority

Section 206 of the USA PATRIOT Act amends FISA to allow the FISC to issue a "generic" secondary order where the Court finds that the "actions of the target of the application may have the effect of thwarting the identification of a specified person." This means that, when a FISA target engages in conduct that has the effect of defeating electronic surveillance, such as by rapidly switching cell phones, Internet accounts, or meeting venues, the Court can issue an order directing "other persons," to effect the authorized electronic surveillance.

Changes in the Duration of FISA Authority

Section 207 of the Act extends the standard duration for several categories of FISC Orders. First, the section allow for electronic surveillances and search orders on non-US person agents of a foreign power pled under Section 101(b)(1)(A) of the FISA, to run for an initial period of 120 days, instead of 90, and to be renewed for periods of one year. The section also extends the standard duration of physical search orders in all other cases, which applies to US persons and non-officer/employee targets, from 45 to 90 days. These extension provisions have resulted in a more effective utilization of available personnel resources and the collection mechanisms authorized under the FISA.

Expansion of the FISC

Section 207 also expanded the FISC from seven judges to eleven judges, three of whom must reside in the Washington, D.C. area. This has increased the availability of FISC judges and has resulted in the convening of the FISC on a weekly basis, which has enabled the FBI to implement FISA-authorized collection operations in a more timely fashion.

Changes in FISA Pen Register/Trap and Trace Authority

Section 214 of the Act makes a substantial revision to the standard for a FISA-authorized pen register/trap and trace. Prior to the USA PATRIOT Act, FISA-authorized pen registers required two showings: (1) relevance to an investigation, and (2) specific and articulable facts giving reason to believe that the targeted line was being used by an agent of a foreign power, or was in communications with such an agent, under specified circumstances. Section 214 simply eliminates the second of the required showings. FISA-authorized pen/trap and trace orders are now available whenever the FBI certifies that "the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."

This new standard requires that the information sought be relevant to an "ongoing investigation to protect against international terrorism or clandestine intelligence activities." Use of this technique is authorized in full investigations properly opened under the AG Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations. Finally, the new standard does not mean that FISA pen register/trap and trace authority is only available on the subjects of investigations. The authority is available when the information sought is "relevant" to the investigation, as described above. For example, information concerning apparent associates or, or individuals in contact with, the subject of an investigation, may be relevant.

Conclusion

The USA PATRIOT Act has provided the FBI with improved tools for conducting counterterrorism and counterintelligence investigations. These new tools require DOJ and the FBI to gain a complete understanding of the provisions, develop guidelines and protocols for their appropriate use, and educate investigators and prosecutors. In addition, many of the provisions require the Department of Treasury to issue new

regulations and rules. While all of this is being done as expeditiously as possible, the full impact of the tools provided by the USA PATRIOT Act are yet to be seen. The FBI is continuing to digest its provisions, develop guidelines and protocols for its appropriate use, and educate investigators and prosecutors. Nevertheless, the Act enhances the ability of law enforcement and intelligence agencies to achieve our common goal of preventing acts of terrorism, without compromising the civil liberties and Constitutional protections enjoyed by our citizens. Thank you for this opportunity to appear today. I welcome any questions you have.

| 2002 Congressional Statement | FBI Home Page |

Office of the Deputy Attorney General
Washington, D.C. 20530

February 6, 2003

MEMORANDUM FOR ALL HOLDERS OF THE UNITED STATES ATTORNEYS' MANUAL

FROM: THE DEPUTY ATTORNEY GENERAL

United States Attorneys' Manual Staff
Executive Office for United States Attorneys

SUBJECT: Criminal Division Approval of Pen Registers and Trap and Trace Applications Involving the Collection of Uniform Resource Locators (URLs)

AFFECTS: All Titles with Criminal Prosecutions
(Titles 3, 4, 5, 6, 7, 8, 9)

The following creates a new section, 9-7.500 (Prior Consultation with the Computer Crime and Intellectual Property Section of the Criminal Division for Applications for Pen Register Orders Capable of Collecting Uniform Resource Locators (URLs)), to Title 9 (Criminal) of the United States Attorneys' Manual, with reference at 9-2.400 (Prior Approvals/Notification table). The new policy similarly has an impact on other titles in regard to their criminal prosecutions and notification/authorization tables. The new section sets forth policy regarding the requirement of prior consultation with the Computer Crime and Intellectual Property Section of the Criminal Division of certain applications for pen register orders.

9-7.500 Prior Consultation with the Computer Crime and Intellectual Property Section of the Criminal Division (CCIPS) for Applications for Pen Register and Trap and Trace Orders Capable of Collecting Uniform Resource Locators (URLs)

In 2001, the USA PATRIOT Act (P.L. 107-56) amended the Pen Register and Trap and Trace Statute (pen/trap statute), 18 U.S.C. § 3121 *et seq.*, to clarify that courts may issue pen/trap orders to collect the non-content information associated with Internet communications. One issue that has been raised in this regard is whether a pen register order may be used to collect (URLs), the terms that a person uses to request information on the World Wide Web (e.g., www.cybercrime.gov/PatriotAct.htm). Because of privacy and other concerns relating to the use of pen register orders in this fashion, use of pen registers to collect all or part of a URL is prohibited without prior consultation with CCIPS. Among the factors that should be considered in deciding whether to apply for such a pen register are (1) the investigative need for the pen register order, (2) the litigation risk in the individual case, (3) how much of any given URL would be obtained, and (4) the impact of the order on the Department's policy goals.

11

Consultation with CCIPS can help resolve these issues, as well as ensuring that the contemplated use of a pen register would be consistent with the Deputy Attorney General's May 24, 2002 Memorandum on "Avoiding Collection and Investigative Use of 'Content' in the Operation of Pen Registers and Trap and Trace Devices."

This policy does not apply to applications for pen register orders that would merely authorize collection of Internet Protocol (IP) addresses, even if such IP addresses can be readily translated into URLs or portions of URLs. Similarly, this policy does not apply to the collection, at a web server, of tracing information indicating the source of requests to view a particular URL using a trap and trace order.

No employee of the Department will use the pen register authority to collect URLs without first consulting with the CCIPS of the Criminal Division. Absent emergency circumstances, such an employee will submit a memorandum to CCIPS that contains (a) the basic facts of the investigation, (b) the proposed application and order, (c) the investigative need for the collection of URLs, (d) an analysis of the litigation risk associated with obtaining the order in the context of the particular case, and (e) any other information relevant to evaluating the propriety of the application. In an emergency, such an employee may telephone CCIPS at (202) 514-1026 or, after hours at (202) 514-5000, and be prepared to describe the above information.

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

May 13, 2003

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

Dear Mr. Chairman:

Thank you for your letter of April 1, 2003, co-signed by Ranking Member Conyers, which posed several questions to the Department on USA PATRIOT Act implementation and related matters. An identical response will be sent to Congressman Conyers.

Pursuant to your request, on April 9, 2003, we notified the Committee that we had forwarded questions number 18, 19, 22, 23, 24, 31, 32 and 26, relating to the authority or operations of the Immigration and Naturalization Service, to the Department of Homeland Security for response. With this letter, we are pleased to transmit responses to the remaining questions.

While we have made every effort to answer each question thoroughly and in an unclassified format, four of the questions will require the submission of classified information. The answer to a portion of question 16(a), and questions 30 and 37 are classified and will be delivered to the Committee under separate cover. In accordance with the direction provided in the Committee's letter of April 1, 2003, and the longstanding Executive branch practices on the sharing of operational intelligence information with the Congress, the classified answers to question 1(c), and a further portion of question 16(a), will be delivered to the House Permanent Select Committee on Intelligence.

We appreciate the opportunity to provide the Committee with information on the Department's efforts in the war on terrorism. If we may be of further assistance on this, or any other matter, please do not hesitate to contact this office.

Sincerely,

Jamie E. Brown

Jamie E. Brown
Acting Assistant Attorney General

Enclosures

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

May 13, 2003

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

Dear Congressman Conyers:

Thank you for your letter of April 1, 2003, co-signed by Chairman Sensenbrenner, which posed several questions to the Department on USA PATRIOT Act implementation and related matters. An identical response will be sent to Chairman Sensenbrenner.

Pursuant to your request, on April 9, 2003, we notified the Committee that we had forwarded questions number 18, 19, 22, 23, 24, 31, 32 and 26, relating to the authority or operations of the Immigration and Naturalization Service, to the Department of Homeland Security for response. With this letter, we are pleased to transmit responses to the remaining questions.

While we have made every effort to answer each question thoroughly and in an unclassified format, four of the questions will require the submission of classified information. The answer to a portion of question 16(a), and questions 30 and 37 are classified and will be delivered to the Committee under separate cover. In accordance with the direction provided in the Committee's letter of April 1, 2003, and the longstanding Executive branch practices on the sharing of operational intelligence information with the Congress, the classified answers to question 1(c), and a further portion of question 16(a), will be delivered to the House Permanent Select Committee on Intelligence.

We appreciate the opportunity to provide the Committee with information on the Department's efforts in the war on terrorism. If we may be of further assistance on this, or any other matter, please do not hesitate to contact this office.

Sincerely,

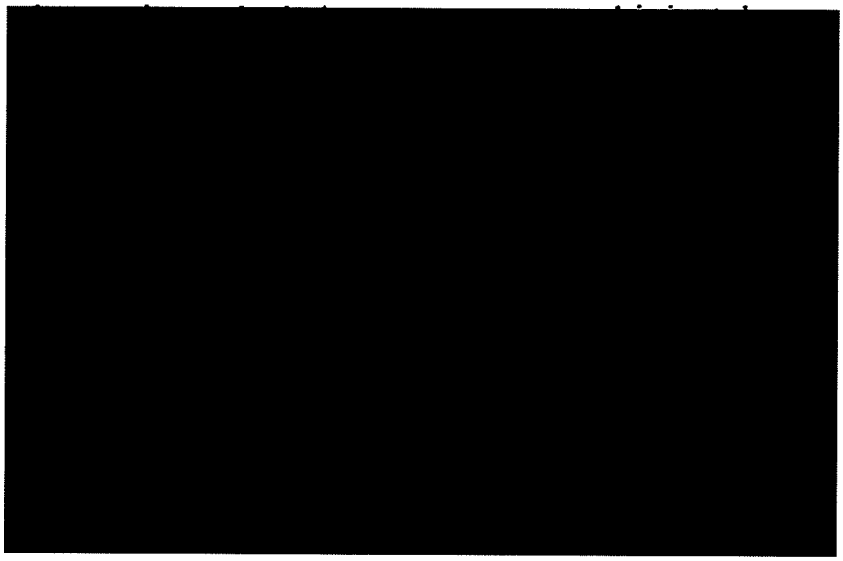
Jamie E. Brown

Jamie E. Brown
Acting Assistant Attorney General

Enclosures

Pages 1-22 are outside the scope of the request

OUTSIDE OF SCOPE



- 216: Amends the pen register/trap and trace statute to clarify that it applies to Internet communications, and gives federal courts authority to authorize the installation and use of pen registers and trap and trace devices in other districts.

  - The Department has used the newly-amended pen/trap statute to track the communications of (1) terrorist conspirators, (2) at least one major drug distributor, (3) thieves who obtained victims' bank account information and stole the money, (4) a four-time murderer, and (5) a fugitive who fled on the eve of trial using a fake passport.

  - This new authority was employed in the investigation of the murder of journalist Daniel Pearl to obtain information that proved critical to identifying some of the perpetrators.

  - The Deputy Attorney General has issued a memorandum to field offices clearly delineating Department policy regarding the avoidance of "overcollection," the inadvertent collection of "content" when using pen/trap devices. This guidance will help protect the privacy of Internet users by ensuring that only addressing information, and not the content of their communications, is collected and used pursuant to section 216. (A copy of this memorandum is attached.)[3]

[3]Attachment D.

Pages 24-60 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

July 31, 2003

The Honorable Steve Chabot
Chairman
Subcommittee on the Constitution
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

We have enclosed responses to written questions posed to the Department following the appearance before the Subcommittee of then-Assistant Attorney General Viet Dinh on May 20, 2003. The subject of the hearing was oversight of the USA PATRIOT Act.

We hope these responses are helpful to you. Please do not hesitate to call upon us if we may be of additional assistance.

Sincerely,

William E. Moschella
Assistant Attorney General

Enclosure

cc: The Honorable Jerrold Nadler
Ranking Minority Member

Responses to Questions by Congressman Steve Chabot
to Assistant Attorney General Viet D. Dinh

OUTSIDE OF SCOPE

[redacted]

OUTSIDE OF SCOPE

OUTSIDE OF SCOPE

[redacted]

[redacted]

[redacted]

Question: Under the USA PATRIOT Act's amendments to the Pen Register Statutes, is it your understanding that all non-"content" information is "dialing, routing, addressing, and signaling" information under 18 U.S.C. § 3127(3), so that all such "dialing, routing, addressing, and signaling" information can be gathered only under the authority of the Pen Register Statute? Or is there a third category of information outside of "contents" (defined in 18 U.S.C. § 2510(8)) and "dialing, routing, addressing and signaling" information, such that its collection by the government falls under neither the authority of the Pen Register Statutes nor the Wiretap Act (which require the government to obtain a warrant to gather the "contents" of communications)? If there is such a third category of information, what statutory provisions or Department rules and procedures govern its collection by the Department of Justice?

Response: The Department of Justice interprets the phrase "dialing, routing, addressing, and signaling information," which is used throughout the pen register and trap and trace statute (18 U.S.C. §§ 3121 et seq.), as complementary to the term "contents," as defined in section 2510(8) of the Wiretap Act. Thus, where law enforcement seeks court authorization

to obtain the "contents" of a communication, it may not do so under the auspices of the pen/trap statute, but rather under the authority of the Wiretap Act. Further, we do not believe that there exists a third category of information which is not comprehended by either "contents" or "dialing, routing, addressing, and signaling information."

OUTSIDE OF SCOPE

[redacted]

Brand, Rachel

From: Hur, Robert
Sent: Friday, April 23, 2004 10:50 AM
To: Brand, Rachel
Cc: Berry, Matthew (OLP)
Subject: RE: Question for CRM

Importance: High

(b)(5) per Criminal Division

Rachel,

I just spoke to Mark Eckenwiler. [redacted]

Exemption (b)(5)

Here's an excerpt from Viet Dinh's testimony before the House Judiciary Committee in May 20, 2003, [redacted] the Q:

Exemption (b)(5)

> Mr. NADLER. Okay, thank you. Mr. Dinh, could you tell us what you consider to be the difference between content and not con—and non-content information in electronic communications? Do you have the technical means to segregate address lines from subject lines in an e-mail? How is this done, and how do you handle URL addresses?
> Mr. DINH. Yes, yes, and that's a hard question. We consider noncontent to be the To and From. The subject line is content. The— we have specified programs that are very precise in their parameters of what they will take and what they will not take. Congress recognized the existence of these programs by—when it enacted section 215, by requiring the Department to use the best available means in order to minimize non-content or excessive, or excessive take. With respect to URLs, the Deputy Attorney General has issued a memorandum, which has been provided to this Committee, on the use of post-cut-through intercepts in the analog world, and also content information in the digital world.

[redacted]

Exemption (b)(5)

(b)(5) per Criminal Division

19

Hepe this is helpful. Good luck. Both Mark Eckenwiler [redacted] and I are around to help if you need to call.

Rob
[redacted] (cell)

Exemption (b)(6)

-----Original Message-----
From: Brand, Rachel
Sent: Thursday, April 22, 2004 5:43 PM
To: Berry, Matthew (OLP)
Cc: Brand, Rachel
Subject: Question for CRM

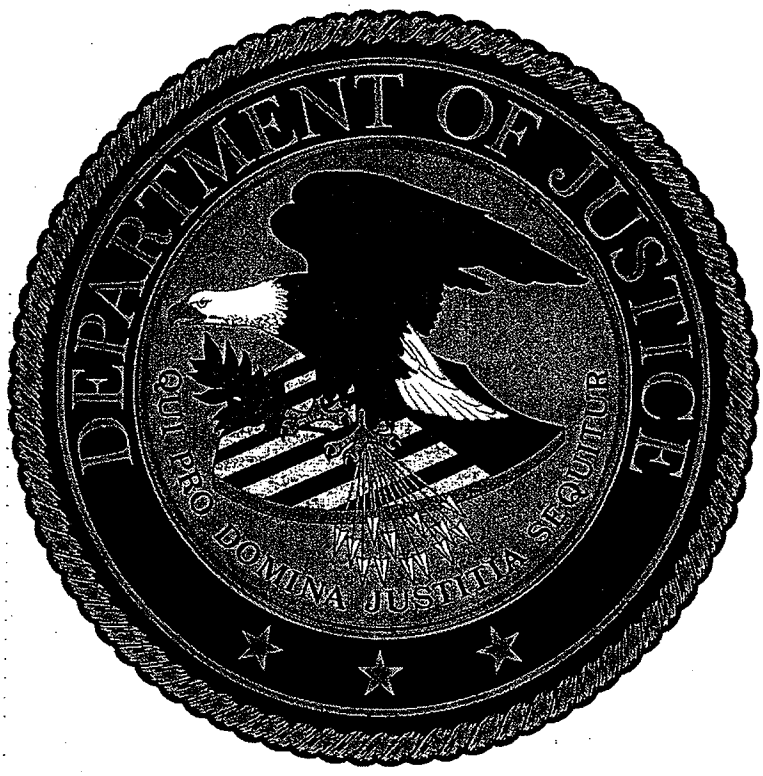
Matthew, I wanted to email a question to rob hur, but his address isn't in my blackbery for some reason. Could you forward this?

[redacted]

Exemption (b)(5)

U.S. Department of Justice

REPORT FROM THE FIELD:
THE USA PATRIOT ACT AT WORK



JULY 2004

Table of Contents

I. Introduction

Immediately after the brutal terrorist attacks of September 11, 2001, both Congress and the Administration reexamined the legal tools available to investigators and prosecutors in the fight against terrorism. Taking into account the lessons learned from past experience, they found these tools to be inadequate. Acting swiftly and responsibly to correct numerous deficiencies, Congress and the Administration set out to update, strengthen, and expand laws governing the investigation and prosecution of terrorism within the parameters of the Constitution and our national commitment to the protection of civil rights and civil liberties. As a result of those efforts, Congress overwhelmingly passed, and on October 26, 2001, the President signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act" or "Act").[1] This legislation provided our nation's law enforcement, national defense, and intelligence personnel with enhanced and vital new tools to bring terrorists and other dangerous criminals to justice. As President Bush stated upon its signing, the Act "takes account of the new realities and dangers posed by modern terrorists. It will help law enforcement to identify, to dismantle, to disrupt, and to punish terrorists before they strike."[2]

The USA PATRIOT Act equips federal law enforcement and intelligence officials with the tools they need to mount an effective, coordinated campaign against our nation's terrorist enemies. The Act revised counterproductive legal restraints that impaired law enforcement's ability to gather, analyze, and share critical terrorism-related intelligence information. The Act also updated decades-old federal laws to account for the technological breakthroughs seen in recent years. For example, terrorists routinely use cell phones to plot their atrocities; under the Act, law enforcement and intelligence officials are no longer hindered by statutes written in the era of rotary telephones. Finally, the Act enhanced America's criminal laws against terrorism, in some cases increasing the penalties for planning and participating in terrorist attacks and aiding terrorists. The Act also clarified that existing laws against terrorism apply to the new types of attacks planned by al Qaeda and other international terrorist organizations.

Since the USA PATRIOT Act was enacted, the Department of Justice – ever cognizant of civil liberties – has moved swiftly and vigorously to put its new tools into practice. As of May 5, 2004, the Department has charged 310 defendants with criminal offenses as a result of terrorism investigations since the attacks of September 11, 2001, and 179 of those defendants have already been convicted. This report provides an overview of how the Act has been instrumental in the effort to combat terrorism and make Americans safer. As described above, the report focuses on the four key areas in which the Act has had the greatest impact: (1) enhancing the federal government's capacity to share intelligence; (2) strengthening the criminal laws against terrorism; (3) removing obstacles to investigating terrorism; and (4) updating the law to reflect

---

[1] Pub. L. No. 107-56, 115 Stat. 272 (2001).

[2] *See Remarks by the President at Signing of the Patriot Act*, October 26, 2001, *available at* http://www.whitehouse.gov/news/releases/2001/10/20011026-5.html.

new technology. The Department has used these improvements in the law to better combat terrorism and continues to work to enhance the coordination, information sharing, and other investigative efforts the USA PATRIOT Act has made possible. Some of the examples in this report do not involve terrorism but instead detail how the Department has used certain provisions in the USA PATRIOT Act to combat serious criminal conduct, such as child pornography and kidnapping. Congress chose not to limit certain authorities contained in the USA PATRIOT Act only to the context of terrorism, and the examples contained in this report demonstrate the wisdom of that decision. Of course, where Congress did choose to limit USA PATRIOT Act authorities to the terrorism or national-security context, the Department has limited the use of those authorities as required by the Act.

For a variety of reasons, this report cannot describe every case in which the USA PATRIOT Act has been instrumental. Some of these cases, for instance, are ongoing and cannot be publicly discussed. Others, particularly including a number of terrorism-related cases, cannot be discussed usefully without disclosing classified information. Therefore, this report is not a comprehensive discussion of the use of USA PATRIOT Act authorities, but is instead an unclassified overview of the usefulness of those authorities.

As the Attorney General has affirmed, "The fight against terrorism is now the first and overriding priority of the Department of Justice."[3] The Department's efforts over the past two-and-a-half years have been characterized by an unwavering commitment to two complementary objectives: securing the United States against the threat of terrorist attacks and preserving the rights and liberties that are guaranteed to every American. Security and liberty are interrelated and mutually reinforcing, not conflicting, goals. Under the leadership of the President and the Attorney General, the Department of Justice has been, and remains, dedicated to using the USA PATRIOT Act in service of both aims.

II. Enhancing the Federal Government's Capacity to Share Intelligence

The USA PATRIOT Act authorizes government agencies to share intelligence so that a complete mosaic of information can be compiled to understand better what terrorists might be planning and to prevent attacks. Prior law, as interpreted and implemented, had the effect of sharply limiting the ability of law enforcement and intelligence officers to share information, which severely hampered terrorism investigators' ability to "connect the dots." However, the USA PATRIOT Act, along with changes in Attorney General Guidelines and Foreign Intelligence Surveillance Act (FISA) court procedures, brought down this "wall" separating intelligence from law enforcement and greatly enhanced foreign intelligence information sharing among federal law enforcement and national security personnel, intelligence agencies, and other entities entrusted with protecting the nation from acts of terrorism. This increased ability to

---

[3] *See Prepared Remarks for the U.S. Mayors Conference*, October 25, 2001, *available at* http://www.usdoj.gov:80/ag/speeches/2001/agcrisisremarks10_25.htm.

share information has been invaluable to the conduct of terrorism investigations and has directly led to the disruption of terrorist plots and numerous arrests, prosecutions, and convictions in terrorism cases.

The recent investigation and prosecution of members of an al Qaeda cell in Lackawanna, New York illustrates the benefits of the increased information sharing brought about by the USA PATRIOT Act. This case involved several residents of Lackawanna, who traveled to Afghanistan in 2001 to receive training at an al Qaeda-affiliated camp near Kandahar. The investigation of the "Lackawanna Six" began during the summer of 2001, when the FBI received an anonymous letter indicating that these six individuals and others might be involved in criminal activity and associating with foreign terrorists. The FBI concluded that existing law required the creation of two separate investigations in order to retain the option of using FISA: a criminal investigation of possible drug crimes and an intelligence investigation related to terrorist threats. Over the ensuing months, two squads carried on these two separate investigations simultaneously, and there were times when the intelligence officers and the law enforcement agents concluded that they could not be in the same room during briefings to discuss their respective investigations with each other.

The USA PATRIOT Act, however, took down the "wall" separating these two investigations by making clear that the sharing of case-sensitive information between these two groups was allowed. As a result of key information shared by intelligence investigators, law enforcement agents were able to learn that an individual mentioned in the anonymous letter was an agent of al Qaeda. Further information shared between intelligence and law enforcement personnel then dramatically expedited the investigation of the Lackawanna Six and allowed charges to be filed against these individuals. Five of the Lackawanna Six pleaded guilty to providing material support to al Qaeda, and the sixth pleaded guilty to conducting transactions unlawfully with al Qaeda. These individuals were then sentenced to prison terms ranging from seven to ten years.

Sections 218 and 504

Before the passage of the USA PATRIOT Act, applications for orders authorizing electronic surveillance or physical searches under FISA had to include a certification from a high-ranking Executive Branch official that the purpose of the surveillance or search was to gather foreign intelligence information. As interpreted by the courts and later the Justice Department, this requirement meant that the "primary purpose" of the collection had to be to obtain foreign intelligence information rather than evidence of a crime. Over the years, the prevailing interpretation and implementation of the "primary purpose" standard had the effect of limiting coordination and information sharing between intelligence and law enforcement personnel. Because the courts evaluated the government's purpose for using FISA at least in part by examining the nature and extent of such coordination, the more coordination that occurred, the more likely courts would find that law enforcement, rather than foreign intelligence, had become the primary purpose of the surveillance or search.

During the 1980s, the Department operated under a set of largely unwritten rules that limited to some degree information sharing between intelligence and law enforcement officials. In 1995, however, the Department established formal procedures that more clearly separated law enforcement and intelligence investigations and limited the sharing of information between intelligence and law enforcement personnel more than the law required. The promulgation of these procedures was motivated in part by the concern that the use of FISA authorities would not be allowed to continue in particular investigations if criminal prosecution began to overcome intelligence gathering as an investigation's primary purpose. To be sure, the procedures were intended to permit a degree of interaction and information sharing between prosecutors and intelligence officers, while at the same time ensuring that the FBI would be able to obtain or continue FISA coverage and later use the fruits of that coverage in a criminal prosecution. Over time, however, coordination and information sharing between intelligence and law enforcement investigators became even more limited in practice than was allowed in theory under the Department's procedures. Due both to confusion about when sharing was permitted and to a perception that improper information sharing could end a career, a culture developed within the Department sharply limiting the exchange of information between intelligence and law enforcement officials.

In recent testimony before the Senate Judiciary Committee, Patrick Fitzgerald, U.S. Attorney for the Northern District of Illinois, recounted from personal experience how this "wall" between law enforcement and intelligence personnel operated in practice:

> I was on a prosecution team in New York that began a criminal investigation of Usama Bin Laden in early 1996. The team – prosecutors and FBI agents assigned to the criminal case – had access to a number of sources. We could talk to citizens. We could talk to local police officers. We could talk to other U.S. Government agencies. We could talk to foreign police officers. Even foreign intelligence personnel. And foreign citizens. And we did all those things as often as we could. We could even talk to al Qaeda members – and we did. We actually called several members and associates of al Qaeda to testify before a grand jury in New York. And we even debriefed al Qaeda members overseas who agreed to become cooperating witnesses.
>
> But there was one group of people we were not permitted to talk to. Who? The FBI agents across the street from us in lower Manhattan assigned to a parallel intelligence investigation of Usama Bin Laden and al Qaeda. We could not learn what information they had gathered. That was "the wall."[4]

The USA PATRIOT Act brought down this "wall" separating intelligence officers from law enforcement agents. It not only erased the perceived statutory impediment to more robust information sharing between intelligence and law enforcement personnel, but it also provided the

---

[4] Statement of Patrick Fitzgerald Before the Senate Committee on the Judiciary, October 21, 2003, *available at* http://judiciary.senate.gov/testimony.cfm?id=965&wit_id=2741.

necessary impetus for the removal of the formal administrative restrictions as well as the informal cultural restrictions on information sharing.

Section 218 of the USA PATRIOT Act eliminated the "primary purpose" requirement. Under section 218, the government may conduct FISA surveillance or searches if foreign-intelligence gathering is a "significant" purpose of the surveillance or search, thus eliminating the need for courts to compare the relative weight of the "foreign intelligence" and "law enforcement" purposes of the surveillance or search, and thereby allowing for increased coordination and sharing of information between intelligence and law enforcement personnel. Section 504 buttressed section 218 by specifically amending FISA to allow intelligence officials conducting FISA surveillance or searches to "consult" with federal law enforcement officials to "coordinate" efforts to investigate or protect against international terrorism, espionage, and other foreign threats to national security, and to clarify that such coordination "shall not" preclude the certification of a "significant" foreign intelligence purpose or the issuance of an authorization order by the Foreign Intelligence Surveillance Court.

The Department has moved aggressively to implement sections 218 and 504 of the USA PATRIOT Act and bring down "the wall." Following passage of the Act, the Department adopted new procedures designed to increase information sharing between intelligence and law enforcement officers, which were affirmed by the Foreign Intelligence Surveillance Court of Review on November 18, 2002. The Attorney General also instructed every U.S. Attorney to review intelligence files to discover whether there was a basis for bringing criminal charges against the subjects of intelligence investigations; thousands of files have been reviewed as part of this process. The Attorney General likewise directed every U.S. Attorney to develop a plan to monitor terrorism and intelligence investigations and to ensure that information about terrorist threats is shared with other agencies and that criminal charges are considered in those investigations.

These efforts to increase coordination and information sharing between intelligence and law enforcement officers, which were made possible by the USA PATRIOT Act, have yielded extraordinary dividends by enabling the Department to open numerous criminal investigations, disrupt terrorist plots, bring numerous criminal charges, and convict numerous individuals in terrorism cases.

Examples:

- The removal of the "wall" separating intelligence and law enforcement personnel played a crucial role in the Department's successful dismantling of a Portland, Oregon terror cell, popularly known as the "Portland Seven." Members of this terror cell had attempted to travel to Afghanistan in 2001 and 2002 to take up arms with the Taliban and al Qaeda against United States and coalition forces fighting there. Law enforcement agents investigating that case learned from one member of the terror cell, Jeffrey Battle, through an undercover informant, that before the plan to go to Afghanistan had been formulated, at least one member of the cell had contemplated attacking Jewish schools or synagogues and had even

been casing such buildings to select a target for such an attack. By the time investigators received this information from the undercover informant, they had suspected that a number of other persons besides Battle had been involved in the Afghanistan conspiracy. But while several of these other individuals had returned to the United States from their unsuccessful attempts to reach Afghanistan, investigators did not yet have sufficient evidence to arrest them.

Before the USA PATRIOT Act, prosecutors would have faced a dilemma in deciding whether to arrest Battle immediately. If prosecutors had failed to act, lives could have been lost through a domestic terrorist attack. But if prosecutors had arrested Battle in order to prevent a potential attack, the other suspects in the investigation would have undoubtedly scattered or attempted to cover up their crimes. Because of sections 218 and 504 of the USA PATRIOT Act, however, it was clear that the FBI agents could conduct FISA surveillance of Battle to detect whether he had received orders from an international terrorist group to reinstate the domestic attack plan on Jewish targets and keep prosecutors informed as to what they were learning. This gave prosecutors the confidence not to arrest Battle prematurely while they continued to gather evidence on the other members of the cell. Ultimately, prosecutors were able to collect sufficient evidence to charge seven defendants and then to secure convictions and prison sentences ranging from three to eighteen years for the six defendants taken into custody. Charges against the seventh defendant were dismissed after he was killed in Pakistan by Pakistani troops on October 3, 2003. Without sections 218 and 504 of the USA PATRIOT Act, however, this case likely would have been referred to as the "Portland One" rather than the "Portland Seven."

- The Department shared information pursuant to sections 218 and 504 before indicting Sami Al-Arian and several co-conspirators on charges related to their involvement with the Palestinian Islamic Jihad (PIJ). PIJ is alleged to be one of the world's most violent terrorist outfits. It is responsible for murdering over 100 innocent people, including Alisa Flatow, a young American killed in a bus bombing near the Israeli settlement of Kfar Darom. The indictment states that Al-Arian served as the secretary of the Palestinian Islamic Jihad's governing council ("Shura Council"). He was also identified as the senior North American representative of the PIJ.

  In this case, sections 218 and 504 of the USA PATRIOT Act enabled prosecutors to consider all evidence against Al-Arian and his co-conspirators, including evidence obtained pursuant to FISA that provided the necessary factual support for the criminal case. By considering the intelligence and law enforcement information together, prosecutors were able to create a complete history for the case and put each piece of evidence in its proper context. This comprehensive approach was essential in enabling prosecutors to build their case and pursue the proper charges. The trial in this case is currently scheduled to start in January 2005.

- Prosecutors and investigators also used information shared pursuant to sections 218 and 504 of the USA PATRIOT Act in investigating the defendants in the so-called "Virginia Jihad" case. This prosecution involved members of the Dar al-Arqam Islamic Center, who trained for jihad in Northern Virginia by participating in paintball and paramilitary training, including eight individuals who traveled to terrorist training camps in Pakistan or Afghanistan between 1999 and 2001. These individuals are associates of a violent Islamic extremist group known as Lashkar-e-Taiba (LET), which primarily operates in Pakistan and Kashmir and has ties to the al Qaeda terrorist network. As the result of an investigation that included the use of information obtained through FISA, prosecutors were able to bring charges against these individuals. Six of the defendants have pleaded guilty, and three were convicted at trial in March 2004 of charges including conspiracy to levy war against the United States and conspiracy to provide material support to the Taliban. These nine defendants received sentences ranging from a prison term of four years to life imprisonment.

- The information sharing between intelligence and law enforcement personnel made possible by sections 218 and 504 of the USA PATRIOT Act was useful in the investigation of two Yemeni citizens, Mohammed Ali Hasan Al-Moayad and Mohshen Yahya Zayed, who were charged last year with conspiring to provide material support to al Qaeda and HAMAS. The complaint against these two individuals alleges that an FBI undercover operation developed information that Al-Moayad had boasted that he had personally handed Usama Bin Laden $20 million from his terrorist fund-raising network and that Al-Moayad and Zayed flew from Yemen to Frankfurt, Germany in 2003 with the intent to obtain $2 million from a terrorist sympathizer (portrayed by a confidential informant) who wanted to fund al Qaeda and HAMAS. During their meetings, Al-Moayad and Zayed specifically promised the donor that his money would be used to support HAMAS, al Qaeda, and any other mujahideen, and "swore to Allah" that they would keep their dealings secret. Al-Moayad and Zayed were extradited to the United States from Germany in November 2003 and are currently awaiting trial.

- The Department used sections 218 and 504 to gain access to intelligence, which facilitated the indictment of Enaam Arnaout, the Executive Director of the Illinois-based Benevolence International Foundation (BIF). Arnaout conspired to obtain charitable donations fraudulently in order to provide financial assistance to Chechen rebels and organizations engaged in violence and terrorism. Arnaout had a long-standing relationship with Usama Bin Laden and used his charity organization both to obtain funds illicitly from unsuspecting Americans for terrorist organizations, such as al Qaeda, and to serve as a channel for people to contribute money knowingly to such groups. Arnaout ultimately pleaded guilty to a racketeering charge, admitting that he diverted thousands of dollars from BIF to support Islamic militant groups in Bosnia and Chechnya. He was sentenced to over 11 years in prison.

- The broader information sharing and coordination made possible by sections 218 and 504 of the USA PATRIOT Act assisted the prosecution in San Diego of several persons involved in an al Qaeda drugs-for-weapons plot, which culminated in several guilty pleas. Two defendants admitted that they conspired to distribute approximately five metric tons of hashish and 600 kilograms of heroin originating in Pakistan to undercover United States law enforcement officers. Additionally, they admitted that they conspired to receive, as partial payment for the drugs, four "Stinger" anti-aircraft missiles that they then intended to sell to the Taliban, an organization they knew at the time to be affiliated with al Qaeda. The lead defendant in the case is currently awaiting trial.

- Sections 218 and 504 were critical in the successful prosecution of Khaled Abdel Latif Dumeisi, who was convicted by a jury in January 2004 of illegally acting as an agent of the former government of Iraq, as well as two counts of perjury. Before the Gulf War, Dumeisi passed information on Iraqi opposition members located in the United States to officers of the Iraqi Intelligence Service stationed in the Iraqi Mission to the United Nations. During this investigation, intelligence officers conducting surveillance of Dumeisi pursuant to FISA coordinated and shared information with law enforcement agents and prosecutors investigating Dumeisi for possible violations of criminal law. Because of this coordination, law enforcement agents and prosecutors learned from intelligence officers of an incriminating telephone conversation that took place in April 2003 between Dumeisi and a co-conspirator. This phone conversation corroborated other evidence that Dumeisi was acting as an agent of the Iraqi government and provided a compelling piece of evidence at Dumeisi's trial.

Section 203

Other provisions of the USA PATRIOT Act besides sections 218 and 504 have also facilitated the sharing of information between law enforcement and intelligence personnel. Before the USA PATRIOT Act, for example, federal law was interpreted generally to prohibit federal prosecutors from disclosing federal grand jury and wiretap information (including "wire, oral, or electronic communications") to intelligence and national defense officials even if that information indicated that terrorists were planning a future attack, unless such officials were assisting with the criminal investigation itself. Sections 203(a) and 203(b) of the USA PATRIOT Act, however, now allow for the dissemination of that information to assist federal law enforcement, intelligence, protective, immigration, national defense, and national security officials in the performance of their official duties, such as protecting the nation's security, even if their duties are unrelated to the criminal investigation. Section 203(d) further specifies that any foreign intelligence information obtained by investigators and prosecutors as part of a criminal investigation may be disclosed to such officials. The Department has made disclosures of vital information to the intelligence community and other federal officials under section 203 on many occasions. For instance, such disclosures have been used to support the revocation of visas of suspected terrorists and prevent their reentry into the United States, track terrorists' funding sources, and identify terrorist operatives overseas.

The Attorney General issued guidelines in 2002 that establish procedures for carrying out these sharing provisions including, under section 203(c), for sharing grand jury and wiretap information that identifies a United States person with the Intelligence Community. These guidelines provide important safeguards to United States citizens identified in information disclosed to the Intelligence Community under the USA PATRIOT Act. These procedures require that precautions are taken to ensure the information is used appropriately. All such information must be labeled by law enforcement agencies before disclosure to intelligence agencies and must be handled by intelligence agencies pursuant to specific protocols.

Section 905

Additionally, section 905 of the USA PATRIOT Act requires all federal law enforcement agencies to disclose expeditiously to the Director of Central Intelligence any foreign intelligence acquired in the course of a criminal investigation. Section 905 makes such information sharing mandatory unless the Attorney General, after consultation with the Director of Central Intelligence, determines that disclosure of certain foreign intelligence would jeopardize an ongoing law enforcement investigation or impair other significant law enforcement interests. On September 23, 2002, the Attorney General released guidelines that formalized the sharing procedures and mechanisms for the Department of Justice and other federal law enforcement agencies that acquire foreign intelligence in the course of a criminal investigation.

III. Strengthening the Criminal Laws Against Terrorism

The USA PATRIOT Act is one aspect of the Department's overarching strategy to remove terrorists from the streets. The Department aims to use its prosecutorial discretion – investigating, prosecuting, and punishing crimes that in the past might have been overlooked – in order to incapacitate suspected terrorists and thereby prevent terrorist attacks. The Act has enhanced the Department's ability to pursue this strategy by strengthening the nation's criminal laws against terrorism, providing the Department with a solid foundation to pursue what has become the Department's highest priority.

For example, before the Act, it was a federal crime to provide material support to individuals or organizations that commit various terrorism crimes. The definition of "material support," however, did not clearly include providing expert advice and assistance – for example, a civil engineer's advice on how to destroy a building or a biochemist's advice on how to make a biological agent more lethal. The law also did not explicitly state that providing "monetary instruments" to a designated foreign terrorist organization constituted material support. Section 805 of the USA PATRIOT Act bolstered the ban on providing material support to terrorists by clearly making it a crime to provide terrorists with "expert advice or assistance" and by clarifying that "material support" includes all forms of money, not just hard currency. In addition, section 810 increased the maximum penalty for providing material support to a terrorist or a terrorist organization from 10 years to 15 years in prison. The Department has successfully used the material support statute in a number of recent cases, such as those involving terror cells in Lackawanna, New York and Virginia. Between September 11, 2001 and May 5, 2004, the

Department charged over 50 defendants with material support offenses in 17 different judicial districts.

Terrorist Financing

The USA PATRIOT Act also strengthened the criminal laws against terrorism by making it easier to prosecute those responsible for funneling money to terrorists. Under previous federal law, 18 U.S.C. § 1960, those who operated unlicensed money transmitting businesses were entitled to rely on the affirmative defense that they had no knowledge of applicable state licensing requirements. Some of these businesses, called hawalas, have funneled extensive amounts of money to terrorist groups abroad. Section 373 of the USA PATRIOT Act amended federal law by eliminating this loophole requiring that the defendant know about state licensing requirements and also by broadening the statute to make it illegal for a person to transmit or transport funds that are the proceeds of criminal activity or funds that are intended to be used for criminal activity. This improved statute has been used in numerous federal prosecutions.

Examples:

- Prosecutors in Florida used section 373 to charge Libardo Florez-Gomez, a money courier who, based upon documentation found on his person, was suspected of laundering an estimated $1.3 million per month for the Revolutionary Armed Forces of Colombia ("FARC"), a leftist rebel group designated by the State Department as a foreign terrorist organization. After intercepting him at the Miami International Airport with $182,000 in euros, U.S. Immigration & Customs Enforcement agents learned during an interview with Florez-Gomez that he intended to convert the euros to dollars in Miami and then transfer them to unknown bank accounts. Because Florez-Gomez was in the business of money transmission, he was arrested and charged with being an unlicensed money transmitter in violation of 18 U.S.C. § 1960, as amended by section 373 of the USA PATRIOT Act. On April 3, 2003, Florez-Gomez pleaded guilty and was subsequently sentenced to serve 18 months in prison, followed by two years of supervised release, and required to forfeit $151,000. In this case, the U.S. Immigration & Customs Enforcement agent who investigated Florez-Gomez was familiar with the statutory registration requirements for money transmitting, which prompted him to focus his interrogation of Florez-Gomez on details pertinent to that violation and not on the elusive element of Florez-Gomez's "knowledge" of the registration requirements – as would have been required prior to enactment of the USA PATRIOT Act.

- Prosecutors in New Jersey have used section 373 of the USA PATRIOT Act to bring charges against Yehuda Abraham, an unlicensed money transmitter whose services were used by Hemant Lakhani, an individual attempting to sell shoulder-fired surface-to-air missiles to terrorists with the understanding that they were going to be used to shoot down American commercial airliners. Lakhani employed Abraham's money transmitting services to funnel, from the United

States to an overseas account, money being paid by a cooperating witness, acting under the direction of federal law enforcement officers, as a down payment on the first missile. As a result of the USA PATRIOT Act, prosecutors were able to quickly put together an effective case against Abraham for operating an unlicensed money transmitting business, avoiding the often fatal issues that plagued such cases prior to the passage of the USA PATRIOT Act. As a result of the strength of the case against him, Abraham entered a plea of guilty to a violation of 18 U.S.C. § 1960 on March 30, 2004. At sentencing, Abraham could receive up to 37 months imprisonment and a $250,000 fine.

- Prosecutors have also secured convictions of individuals operating unlicensed money transmitting businesses that sent money from the United States to Iraq, Yemen, the United Arab Emirates, and India. In Boston, for example, the successful prosecution of Mohammed Hussein, the co-operator of an al-Barakaat-affiliated money transmitting business, was based on both pre- and post-USA PATRIOT Act violations of 18 U.S.C. § 1960. In 2000 and 2001, Barakaat accepted approximately $3 million in customer deposits and wired those funds to the United Arab Emirates without a license. Based on those transactions, Hussein was sentenced on July 22, 2002, to one-and-a-half years in prison, to be followed by two years of supervised release.

Forfeiture

In an effort to stem the flow of money to terrorists, section 371 of the USA PATRIOT Act made bulk cash smuggling a serious criminal offense. Section 371 specifically forbids concealing more than $10,000 in currency or other monetary instruments and transporting it out of or into the United States with the intent to evade relevant reporting requirements. Violators are subject to five years in prison and forfeiture of any property involved in the offense. Prior to the passage of the USA PATRIOT Act, federal law required anyone transporting monetary instruments of more than $10,000 into or out of the country to file a report but did not make currency smuggling itself a crime. The U.S. Supreme Court therefore had ruled that defendants violating that law could not be required, consistent with the Eighth Amendment, to forfeit large amounts of money since the crime was merely a reporting offense. The criminal offense of bulk cash smuggling is designed to remedy this ruling. Prosecutors have used section 371 of the USA PATRIOT Act to obtain the forfeiture of millions of dollars connected with terrorism and drug dealers.

Example:

- Alaa Al-Sadawi, a New Jersey imam with ties to a designated foreign terrorist organization, was charged with and convicted of violating section 371. Al-Sadawi had enlisted the help of his elderly parents in attempting to smuggle $659,000 in cash to Egypt. Specifically, customs agents discovered the currency in a box of Ritz crackers, two boxes of baby wipes, and a box of Quaker Oats inside a suitcase carried by his father on a commercial flight. Previously, this

conduct could only have been prosecuted as a reporting offense, and prosecutors would not have been able to obtain forfeiture of all the unreported currency. Because of section 371 of the USA PATRIOT Act, however, the United States is currently seeking forfeiture of the entire $659,000 that Al-Sadawi was attempting to smuggle out of the country.

In addition to allowing the federal government to obtain greater forfeitures from cash smugglers, section 806 of the USA PATRIOT Act bolstered federal law by expressly making terrorists' property subject to forfeiture. Specifically, the provision authorizes the government to seize property belonging to an individual or entity that plans or engages in domestic or international terrorism against the United States, acquired for use in future terrorist attacks, or representing the fruits of an act of terrorism. Prosecutors in Oregon recently used this provision to seize the assets of three defendants in the case of the Portland, Oregon terror cell discussed above.

Beyond making more assets subject to forfeiture, Congress also provided the Department in the USA PATRIOT Act with a new tool to seize those assets subject to forfeiture under 18 U.S.C. § 981 or under the Controlled Substances Act. Such assets include both terrorism-related assets and various other assets connected with illegal activity. Section 319 authorizes the government to seize funds subject to forfeiture that are located in a foreign bank account by authorizing the seizure of foreign banks' funds that are held in a correspondent U.S. account. This is true regardless of whether the money in the correspondent account is directly traceable to the money held in the foreign bank account. The Department has used section 319 in several significant cases.

Example:

- On January 18, 2001, a federal grand jury indicted James Gibson for offenses including conspiracy to commit money laundering and mail and wire fraud. Gibson had defrauded his clients, who were numerous personal injury victims including widows, orphans, and those in need of expensive medical care, of millions of dollars by fraudulently structuring settlements. Gibson and his wife, who was indicted later, fled to Belize, depositing some of the proceeds from their scheme in two Belizean banks. The Department's efforts to recover the proceeds initially proved unsuccessful. Although Belize's government initially agreed to freeze the money, a Belizean court lifted the freeze and prohibited the government from further assisting American law enforcement agencies. Efforts to break the impasse failed, while the Gibsons systematically drained their accounts in Belize by purchasing luxury items. Following the passage of the USA PATRIOT Act, a seizure warrant was served on the Belizean bank's correspondent account in the United States pursuant to section 319, and the remaining funds were recovered. The government intends to return the recovered $1.7 million to the victims of Gibson's fraud scheme.

Biological Weapons

The USA PATRIOT Act also bolstered criminal laws aimed at preventing terrorist attacks involving biological weapons. Prior to the passage of the USA PATRIOT Act, federal law prohibited the use of biological agents or toxins as a weapon. Recognizing the inherent dangers posed by biological agents or toxins, section 817 of the USA PATRIOT Act broadened the biological weapons statute to ensure that biological agents or toxins are only in the hands of those with a valid reason for having them. In particular, section 817 both outlaws the possession of biological agents or toxins that cannot be justified by a peaceful purpose, such as research, and makes it a federal crime for certain individuals, such as convicted felons, to possess them. Prosecutors in Connecticut have used section 817 to charge a graduate student who was directed to dispose of laboratory samples of anthrax. While he discarded certain samples, the student took other samples and hid them. Although there was no evidence that he planned to use anthrax as a weapon, neither was there any indication that he sought to possess anthrax for a valid peaceful purpose, such as research. In this particular case, the defendant was allowed to complete a pretrial diversion program. But in future cases, section 817 may serve as a valuable weapon in the prosecution of those possessing biological agents or toxins under more suspicious circumstances.

Cyber-terrorism

The USA PATRIOT Act also strengthened criminal laws protecting against cyber-terrorism. Section 814 of the USA PATRIOT Act increased the maximum penalty for intentionally damaging a federally protected computer from a prison term of five years to a prison term of 10 years and raised the maximum penalty from a prison term of 10 years to a prison term of 20 years for intentionally or recklessly damaging a federally protected computer after having previously been convicted of computer abuse.

In section 814, Congress also broadened the scope of protection provided to federally protected computers. Prior to the passage of the USA PATRIOT Act, criminal or civil liability for damaging a federally protected computer was triggered only if the damage fell into one of four categories, such as causing a loss of five thousand dollars or more. Section 814, however, added a fifth category for triggering criminal or civil liability: damage affecting a computer system used by or for the government in furtherance of the administration of justice, national defense, or national security.

Example:

- Prosecutors in Wisconsin recently used this provision of the USA PATRIOT Act in a case involving Rajib Mitra, a man who jammed the Madison, Wisconsin police department's emergency radio system 21 times from January 2003 to August 2003 and for three hours on October 31, 2003, a day on which public safety concerns were heightened because of Halloween. Mitra's conviction in March 2004 was based in part on section 814's extension of protection to

computers used in the administration of justice, national defense, and national security. Mitra was sentenced in May 2004 to a prison term of eight years.

Section 814, furthermore, clarified that the meaning of "loss" under the computer crime statute includes the reasonable costs of responding to the offense, conducting a damage assessment, and other consequential losses from the computer hacking. This change helps ensure that those who intentionally invade and damage computer systems are held responsible for the full economic consequences of their actions.

Mass Transportation Protection

Finally, before the USA PATRIOT Act was passed, the federal prohibition on attacking transportation carriers was a patchwork of federal statutes with gaps that had the potential to hamper terrorism investigations. Section 801 of the Act filled in these gaps by creating a new crime of attacking a mass transportation system. Among other things, it now is illegal to destroy a mass transportation vehicle or place a biological toxin near a mass transportation vehicle. Since the passage of the Act, the Department has used section 801 in at least two cases.

Examples:

- Section 801 was used to prosecute a cruise ship passenger for leaving two threatening notes aboard the cruise liner "Legend of the Seas" during a voyage from Mexico to Hawaii. In these notes, which were left in a restroom aboard the ship, the passenger stated that American passengers and crew members would be killed if the ship, with 1,600 passengers and 700 crew members, ported in the United States. After 120 federal, state, and local law enforcement officers of the Hawaii Joint Terrorism Task Force investigated the threat and searched the ship, it was eventually discovered that the notes were a hoax. Because section 801 was judged most applicable to the situation at hand, the passenger in question was charged with two violations of that provision of the USA PATRIOT Act. She later pleaded guilty to one count and was sentenced to a prison term of two years.

- Prosecutors in California used section 801 of the USA PATRIOT Act to indict a one-time Orange County resident who phoned in from overseas several threats to blow up John Wayne Airport. Because of these threats, parts of the airport were shut down on several occasions, and police department bomb teams and other emergency personnel were called out to the airport several times to investigate the situation. While the perpetrator has not yet been located and arrested, a warrant for his arrest has been issued, and the threats have ceased.

Additionally, the Department attempted to use section 801 in its prosecution of Richard Reid, commonly referred to as the "shoebomber." Reid was arrested on December 22, 2001, after attempting, while aboard an international flight bound for Miami, Florida, to ignite a bomb hidden in his shoes. A federal grand jury indicted Reid on nine charges, including the newly created charge of attempting to destroy a mass transportation vehicle. A federal judge in Boston

later dismissed this charge, concluding that airplanes did not fall within the meaning of "mass transportation vehicle" as that term is defined in section 801 of the USA PATRIOT Act. After the judge's decision was published, however, Congress amended the statute to clarify that aircraft are covered by the provision.

IV. Removing Obstacles to Investigating Terrorism

In addition to facilitating the coordination and sharing of information in terrorism investigations and strengthening the criminal laws against terrorism, the USA PATRIOT Act also removed a number of significant legal obstacles that prevented law enforcement from effectively investigating terrorism and related criminal activity. It has greatly improved the Department's ability to disrupt, weaken, thwart, and eliminate the infrastructure of terrorist organizations, to prevent or thwart terrorist attacks, and to punish perpetrators of terrorist acts.

Frequently, time is of the essence in terrorism investigations, as law enforcement officers may have only a very brief window of opportunity to prevent a terrorist attack. In the past, investigators had to waste precious time petitioning multiple judges in multiple districts for search warrants related to the same case. The USA PATRIOT Act, however, streamlined this process, making out-of-district search warrants available to law enforcement in terrorism cases. Section 219 of the Act now permits a federal judge with jurisdiction over the offense to issue search warrants that can be executed in other specified judicial districts. Section 219 was used in the investigation of eight members of the Palestinian Islamic Jihad later indicted for conspiring to provide material support to a foreign terrorist organization, the individuals prosecuted in the Virginia Jihad case, and the man who drove a tractor onto the National Mall in Washington, D.C. and threatened to detonate a bomb in 2003. Law enforcement has also used this authority on numerous other occasions.

Examples:

- A noteworthy use of section 219 occurred during the ongoing anthrax investigation, when FBI agents applied for a warrant to search the premises of America Media, Inc. in Boca Raton, Florida – the employer of the first anthrax victim. Using section 219, agents were able to obtain a search warrant from the federal judge in Washington, D.C. overseeing the wide-ranging investigation. Investigators saved valuable time by petitioning the local federal judge who was most familiar with the case.

- In 2002, a package intended for a New Jersey man was mistakenly delivered to another person. Inside the package were fraudulent identification documents. Law enforcement investigators learned that the identification documents had been sent by a man in Texas who was found to possess a large quantity of weapons, including chemical weapons such as sodium cyanide. A subsequent search of the New Jersey man's residence revealed many guns and gas masks, numerous knives including those made to avoid setting off a metal detector, a crossbow, and thousands of rounds of ammunition including hollow point and armor piercing

bullets. As a result of section 219, law enforcement agents were quickly able to secure a search warrant in New Jersey for a search of Vermont properties associated with the New Jersey man, rather than having to go through the additional time and effort necessary to secure such a warrant in Vermont. The searches in Vermont subsequently revealed over 10,000 rounds of ammunition and over 70 firearms including an AK-47 gun, an Uzi firearm, and the barrel of a .50-caliber weapon. Investigators believe that their ability to search the Vermont properties quickly was important in the recovery of the weapons and ammunition. The New Jersey man subsequently pleaded guilty to aiding and abetting the transportation of false identification documents.

- The Justice Department recently used section 219 in an investigation that led to the prosecution of several individuals for acting as unregistered agents of the Iraqi intelligence service in 2003 before and during our military action in Iraq. The U.S. Attorney's Office for the Southern District of New York obtained a search warrant from a Magistrate Judge in New York authorizing the search of the premises of a suspect in Maryland who was to be arrested in conjunction with the execution of the search warrant. The suspect was charged with, among other things, participating in illegal financial transactions with a state sponsor of terrorism, specifically Iraq. Prosecutors report that the ability to use section 219 was crucial in coordinating the successful multi-district plan of arresting one of the defendants and executing the search simultaneously. Because of the high-profile nature of the particular defendant, section 219 was also critical to the Department's ability to limit the number of people who had knowledge of the operation prior to its execution, which helped to assure its success. The fruits of the search in Maryland revealed critical additional evidence against the suspect, and she is currently awaiting trial.

In addition to allowing law enforcement to secure evidence quickly against terrorists, section 219 has been useful in enabling authorities to uncover terrorism hoaxes rapidly, thus preventing or minimizing the disruption that such hoaxes cause.

Example:

- Several Atlantic City casinos received a letter on the same day indicating that a chemical or biological agent would soon be released into their ventilation systems. After learning the identity of the sender of these letters, the government obtained a search warrant in New Jersey to authorize the search of a home in Ohio, enabling agents to execute the search warrant within 24 hours of receiving the letters. Once investigators completed their search, they were able to determine that the suspect had sent the letters as a hoax in order to induce the casinos to pay him money later for providing a "tip" about an imminent terrorist incident.

The USA PATRIOT Act has also improved the effectiveness of FISA. Under FISA, a federal court – the United States Foreign Intelligence Surveillance Court ("FISC") – reviews Department requests for physical searches and electronic surveillance of foreign powers and their agents. Under prior law, the Department could only conduct FISA searches of agents of foreign powers for periods lasting up to 45 days prior to having to seek renewal of such authority from the court. That limitation required federal authorities to waste valuable time and resources by frequently renewing court orders, even when there was no question about the legal sufficiency of a particular case. Section 207 of the USA PATRIOT Act now permits the FISC to authorize physical searches of certain agents of foreign powers (including U.S. persons) for 90 days, and authorizes longer periods of searches and electronic surveillance for certain categories of foreign powers and non-U.S. persons who are agents of foreign powers. In particular, for foreign governments and other foreign powers, non-U.S. person officers or employees of certain foreign powers, and non-U.S. person members of international terrorist groups, initial orders authorizing searches and surveillance may be for periods of 120 days, and renewal orders may extend for periods of one year. While the details of FISA operations are classified, the FISC has authorized 90-day and year-long surveillance of foreign powers and their agents pursuant to section 207 of the USA PATRIOT Act. Therefore, the Act has not only provided additional time to government investigators targeting potential terrorist activity, it has also helped the government and the FISC to focus their efforts on more significant and complicated terrorism-related cases.

Coordination is often the key to a successful investigation. Section 506 of the USA PATRIOT Act enables the Justice Department and other agencies to cooperate fully and integrate completely their investigations in certain areas. It does so by extending the jurisdiction of the Secret Service and FBI to investigate computer fraud. It also gives the FBI primary authority to investigate a number of specific computer fraud offenses, including those involving espionage, foreign counterintelligence, and the unauthorized disclosure of national defense information.

The USA PATRIOT Act also enhanced the Department's ability to use DNA technology in terrorism and other criminal investigations. Collecting DNA from terrorists will make it possible to solve crimes by matching their DNA profiles to biological residues found at crime scenes and by including terrorists' DNA in the criminal information databases that are available to law enforcement and immigration officials. Previous federal law did not authorize officials to collect DNA samples from federal prisoners who had been convicted of terrorism offenses, including hijacking an airplane or bombing a building, even though officials could take samples from prisoners convicted of less destructive crimes, such as robbery. Section 503 of the Act removed this loophole by permitting federal officials to take DNA samples from any federal prisoner convicted of a crime of terrorism or violence. The Department issued regulations on December 29, 2003, to implement this additional authority and to enhance further our use of DNA technology in the investigation and prosecution of terrorists.

Another tool that previously was more widely available in common criminal investigations than in terrorism investigations was the use of rewards. Before the USA PATRIOT Act, federal law strictly limited the amounts of rewards the Attorney General could pay to those who help investigators combat acts of terrorism. The State Department's authority

to pay rewards in terrorism investigations similarly was limited. These limitations hampered the government's ability to punish the guilty by limiting incentives that could be offered to gain the support of foreign countries and the general public. Section 501 of the Act abolished these restrictions by authorizing the Attorney General to pay rewards of whatever amount he determines is necessary to combat terrorism. Section 502 of the Act likewise enhanced the State Department's ability to pay rewards in such investigations.

The USA PATRIOT Act also allows law enforcement officials, in limited situations, to access information about suspected criminals who are enrolled in educational institutions. Previous federal law generally prohibited educational institutions from releasing information from student education records without the student's consent – a requirement that impeded the government's efforts to undertake terrorism investigations involving students. Sections 507 and 508 allow for a limited override of this prohibition, by court order, if the educational records contain information related to the investigation of an act of terrorism. They also permit investigators to obtain information from the National Center for Education Statistics. The Department, with assistance from the Secretary of Education, is currently drafting guidelines designed to ensure the confidentiality of educational records that are disclosed under sections 507 and 508.

V. Updating the Law to Reflect New Technology

Prior to the USA PATRIOT Act, law enforcement had been operating at a technological disadvantage in the war against terrorism. Agents often were forced to use outdated legal authorities to fight terrorists who were using modern technology. In short, we were waging a 21st century war with mid-20th century weapons. Thankfully, however, the Act has modernized and strengthened key tools needed to accomplish the Department's now-central mission: preventing acts of terrorism before they take place. The USA PATRIOT Act's modernization of federal law falls into three broad categories. First, the Act gives federal officers new tools to fight terrorists who use modern technologies to plot their attacks. Second, it enhances existing investigative tools, such as wiretaps and pen register and trap and trace ("pen/trap") devices, to bring them up-to-date with changing technology. And third, the USA PATRIOT Act helps officials to obtain the cooperation of third parties, such as communications providers, in the war against terrorism.

Providing New Tools to Fight Terrorists and Criminals Using Electronic Forms of Communications

The USA PATRIOT Act extends our capacity to collect information related to communications in the digital world. Terrorists and other criminals have used the Internet as an easy method of communication. As a result, in section 210 of the USA PATRIOT Act, Congress authorized the use of administrative and grand-jury subpoenas to obtain information about temporarily assigned network addresses and users' billing records from electronic communications service providers without requiring investigators first to undertake the time-consuming step of applying to the courts. (As is true of all subpoenas, recipients of a section 210 subpoena are free to go to court to quash it.) The speedy acquisition of this information has

allowed authorities to identify perpetrators more easily and keep pace with terrorists and other criminals. In addition, it has been extremely helpful in combating the sexual abuse of children.

Examples:

- Section 210 of the USA PATRIOT Act was used to obtain information related to the investigation of a Columbine-like attack that was supposed to occur on a specific date in early March 2004. The information obtained through section 210 was used to identify the suspect quickly. He was then interviewed by the FBI and confessed before any attack could take place.

- In 2003, the Indiana State Police was informed that child pornography portraying a 13-year-old girl from Southern Indiana had been posted to an Internet website. After an initial investigation, investigators suspected the father of the victim as being the offender partially visible in one of the photographs. As a result, taking advantage of the authority provided by section 210 of the USA PATRIOT Act, grand jury subpoenas were issued requesting relevant Internet subscriber information. This information confirmed investigators' suspicion that the victim's father was the perpetrator. Consequently, ten days after the initial report to the Indiana State Police and using the information obtained by the subpoena to the Internet company, a search warrant was executed at the father's home, and numerous items of child pornography were seized. The girl was interviewed and admitted that she was being sexually abused by her father on an ongoing basis and that he was filming and photographing these sexual acts. The father was subsequently arrested and pleaded guilty to five counts of producing child pornography. He was sentenced earlier this year to a prison term of approximately 10 years. By using the authority contained in section 210, Indiana State Police investigators were able to speed up significantly their investigation, thus enabling the girl to be removed from her family's house more quickly and preventing future molestations by her father.

- In Operation Hamlet, U.S. Immigration and Customs Enforcement agents used section 210 to assist in dismantling an international ring of active child molesters, many of whom were molesting their own children. In the process, they rescued more than 100 child victims. The perpetrators photographed and videotaped the abuse and then exchanged it amongst the ring of child molesters over the Internet. In some instances, the abusers molested the children while simultaneously running a "live-feed" via a webcam so that the other molesters could watch the abuse occurring in real-time. In other cases, the abusers traveled to each others' homes so that they could molest the children together. Subpoenas were issued to Internet service providers during the investigation requesting relevant information. With this information, much of which could not have been obtained quickly prior to the USA PATRIOT Act, investigators were able to identify many members of this molestation ring and obtain search and arrest warrants. As a

result, twenty-one people have been indicted in the United States, resulting in nineteen convictions. Two more are awaiting trial.

- In Operation Artus, U.S. Immigration and Customs Enforcement agents, working with the German National Police, used section 210 to assist in dismantling a child pornography group whose aim was to obtain and exchange recently produced child pornography that had not yet been publicly disseminated. The group consisted of approximately 46 individuals exchanging child pornography on the Internet. To be admitted into the group, a prospective member had to demonstrate that he had new, previously unavailable, images of child pornography. Investigators issued subpoenas to Internet service providers during the investigation, requesting relevant information. With this information, investigators were able to identify many of the members of this ring and obtain search and arrest warrants. As a result, 10 participating countries, including the United States, executed search warrants simultaneously in March 2002. To date, there have been 11 searches, eight indictments, and five convictions in the United States as a consequence of this investigation.

- In Kentucky, a multi-agency task force of local, state, and federal law enforcement used section 210 of the USA PATRIOT Act in its investigation of an individual linked to several sexual assaults of children at public libraries and local parks. Just before the individual in question became the primary suspect in the case, he attempted to rape and abduct a six-year-old girl at a playground in Boone County, Kentucky. Once the man was identified as the primary suspect, an informant provided the investigating officers with some information about the suspect. Investigators then used section 210 to subpoena additional key information from an Internet service provider. Within 20 minutes of receipt of the subpoena, the investigative team obtained information that was ultimately a pivotal part of a search warrant affidavit that led to a search of the suspect's residence. Without the information that was obtained pursuant to section 210, it is unlikely that sufficient information would have been available to obtain the search warrant. Evidence located in the house was then used to arrest the suspect and his wife within 24 hours of obtaining the information from the subpoena. The couple was prosecuted pursuant to a 100-count federal indictment for the receipt and possession of child pornography. The federal investigation and prosecution has also led to information tying the couple to multiple sexual assaults in Kentucky and Virginia. The defendants were convicted of the receipt and possession of child pornography and were sentenced to prison terms of approximately 30 years and 90 years respectively.

The USA PATRIOT Act also improved the speed of obtaining search warrants for electronic mail. Prior to the Act, law enforcement's access to vital electronic information was often impeded by the fact that a court sitting in one district could not issue a warrant that was valid in another district. As a result, investigators' access to critical Internet-related information was unnecessarily delayed, as Internet service providers often are located thousands of miles

from the scene of the crime under investigation, and officers were forced to apply for a warrant in the jurisdiction where the search would be conducted. In section 220 of the USA PATRIOT Act, Congress adapted federal law to changing technology by allowing courts to order the release of stored communications through a search warrant valid in another specified judicial district. The enhanced ability to obtain this information efficiently has proved invaluable in several terrorism investigations, such as the Virginia Jihad and "shoebomber" cases described above, as well as time-sensitive criminal investigations, such as the following situation involving a dangerous fugitive.

Example:

- A man, armed with a sawed-off shotgun, abducted his estranged wife and sexually assaulted her. Then, after releasing his wife, he fled West Virginia in a stolen car to avoid capture. While in flight, he continued to contact cooperating individuals by e-mail using an Internet service provider located in California. Using the authority provided by section 220, investigators in West Virginia were able to obtain an order quickly from a federal court in West Virginia for the disclosure of information regarding the armed fugitive's e-mail account, rather than wasting additional time obtaining such an order from a California court. Within a day of the order being issued, the Internet service provider released information to the government revealing that the fugitive had contacted individuals from a public library in a small town in South Carolina. The very next day, Deputy U.S. Marshals went to the town and noticed a carnival set up next to the public library. Since they were aware that the fugitive had previously worked as a carnival worker, the Deputy Marshals went to the carnival and discovered the stolen car. They waited, and then arrested the fugitive as he approached the car. He later pleaded guilty in state court and was sentenced to imprisonment for a term of 30 years. In this case, the fast turn-around on the order for information related to the fugitive's e-mail account, made possible by section 220 of the USA PATRIOT Act, was crucial to capturing the fugitive.

In addition to allowing law enforcement to gain access to information quickly in time-sensitive investigations, Congress also significantly improved the Justice Department's ability to mount large-scale child pornography investigations by including section 220 in the USA PATRIOT Act. The ability to obtain search warrants in the jurisdiction of a child pornography investigation rather than in the jurisdiction of the Internet service provider is critical to the success of a complex, multi-jurisdictional child pornography case. In the absence of section 220, law enforcement agents would either have to spend hours briefing other agents across the country to obtain warrants or travel hundreds or thousands of miles to present a warrant application to a local magistrate judge. In practice, one of two things would often occur in light of limited law enforcement resources: either the scope of the investigation would be narrowed or the case would be deemed impractical at the outset and dropped.

Section 220 has also dramatically reduced the administrative burdens in judicial districts that are home to large Internet service providers. Before the USA PATRIOT Act, these districts

were inundated with search warrant requests for electronic evidence. For example, prior to the passage of the USA PATRIOT Act, the U.S. Attorney's Office in Alexandria, Virginia, was receiving approximately 10 applications each month from United States Attorney's Offices in other districts for search warrants for records from a particular Internet service provider. For each of these applications, an Assistant United States Attorney in Virginia and a law enforcement agent in the district had to learn all of the details of another district's investigation to present an affidavit to the court in support of the application for the search warrant. The result was that agents and attorneys spent many hours each month processing applications for investigations conducted in other districts. Because of section 220, however, these attorneys and agents can now spend their time on more important tasks than processing paperwork for other districts' investigations.

Investigations of terrorism and other crimes have also long been frustrated by the failure of federal law to permit agents to gain access to voice-mail messages with a search warrant. Prior to the USA PATRIOT Act, federal law required officers to waste critical time and resources going through the burdensome process of obtaining a wiretap order (rather than a search warrant) to obtain unopened voice-mail. This was so despite the fact that authorities could use a search warrant, for example, to obtain messages stored on the suspect's own answering machine. Section 209 of the USA PATRIOT Act has modernized federal law by enabling investigators to access more quickly suspects' voice-mail by using a search warrant. The speed with which voice-mail is seized and searched can often be critical to an investigation because stored voice-mail is regularly deleted by service providers and thus lost forever. Warrants pursuant to section 209 have been used to obtain key evidence in a variety of criminal cases, including voice-mail messages left for those participating in a large-scale ecstasy smuggling ring based in the Netherlands.

Since 1986, law enforcement officials have been able to obtain multiple-point wiretaps to keep pace with drug dealers and mobsters who, for example, frequently switch cell phones to evade surveillance. Prior to enactment of the USA PATRIOT Act, such authority was not available under FISA for cases involving terrorists. Section 206 of the Act, however, now permits officers in international terrorism investigations to obtain a court order that applies to the suspect, rather than a particular phone or phone company. This new authority has put investigators in a better position to avoid unnecessary cat-and-mouse games with terrorists, who are trained to thwart surveillance. While particular examples of the use of multiple-point wiretaps pursuant to section 206 remain classified, the following hypothetical illustrates the utility of this authority.

Suppose, for example, that investigators become aware of an al Qaeda plot to launch a bomb attack. Investigators also discover a recent cellular telephone number for the suspected bomber, for which they immediately obtain a FISA surveillance order. When they attempt to begin surveillance of the suspect, however, they discover that he has changed cellular telephone numbers and providers in order to thwart surveillance. Because of section 206, in cases where the subject's actions may have the effect of thwarting the identification of a service provider, investigators can now obtain a FISA multiple-point surveillance order and immediately serve it on the suspected bomber's new cellular provider, allowing undercover agents to monitor his new

cellular telephone number immediately. Without section 206, however, investigators in such cases would be forced to waste valuable time returning to the FISA court just to obtain a new order containing the new provider's name.

Like several of the other technology-related problems that law enforcement faced prior to the enactment of the USA PATRIOT Act, investigators were often delayed or restricted in gaining access to records relating to telephone and Internet services when the provider of those services was a cable company. These delays occurred because of confusion as to whether cable companies, when providing communications as compared to pay television services, would be governed by the Cable Act. The federal Cable Act set out extremely restrictive rules governing access to cable company records, while all other communications providers were clearly subject to search warrants, court orders, and subpoenas. The cable companies, faced with arguably conflicting legal obligations, often sought clarifications from the courts, which delayed and sometimes jeopardized criminal investigations. In one particular case, law enforcement was investigating a suspected pedophile who not only distributed images of child pornography online, but bragged that he was sexually molesting a minor girl. Agents obtained a court order directing the cable company to disclose his name and other information. The cable company refused to comply with the court order, citing restrictions in the Cable Act. Investigators were forced to pursue other leads for two weeks before eventually identifying and arresting the suspect.

Section 211 of the USA PATRIOT Act eliminated this problem by clarifying that federal wiretap and electronic communications statutes, and not the federal Cable Act, govern cable companies' disclosures relating to their customers' use of telephone and Internet services. Cable companies are now subject to search warrants, court orders, and subpoenas to the same extent as all other communications carriers, thereby ensuring that terrorists and other criminals are not exempt from investigations simply because they choose cable companies as their communications providers. The Cable Act, however, continues to protect information related to subscribers' television-viewing habits. This clarification has already proven valuable in several investigations.

Example:

- Section 211, for example, enabled investigators to obtain information that was crucial to identifying an individual who had sent over 200 threatening letters, laced with white powder, to various government agencies, businesses, and individuals in Louisiana. These letters paralyzed the town of Lafayette, Louisiana for days in 2002 as law enforcement agencies with a limited number of Haz-Mat units frantically tried to respond to numerous requests for assistance. The letters also shut down the local post office for 24 hours as well as all local courthouses, many government offices, and scores of local businesses. As a result of information provided by a cable company pursuant to section 211 of the USA PATRIOT Act, the perpetrator was eventually arrested, convicted, and sentenced to a prison term of 30 years.

Enhancing Existing Investigative Tools

To be effective against the tactics used by today's criminals, including terrorists, many existing laws needed only to be updated. For instance, investigators had used "pen/trap" devices for many years to determine the source or destination of communications, such as numbers dialed by, or received by, a particular telephone. When Congress first enacted the law governing the use of pen/trap devices in 1986, however, it could not have anticipated the dramatic expansion in electronic communications that has occurred since then. The statute therefore did not expressly apply to the full range of communications media, such as the Internet. Moreover, the original statute did not address the increasingly mobile nature of communications, and therefore limited the effect of a pen/trap order to the territorial boundaries of the federal district in which it was issued. In Section 216 of the USA PATRIOT Act, Congress amended the pen/trap statute to authorize a district court to issue an order that is valid throughout the United States, and it clarified that the pen/trap provisions in criminal investigations apply to communications via means other than telephones, such as the Internet.

With this new tool, officials no longer have to apply for new orders each time an investigation leads to another judicial district and may trace terrorists' and other criminals' communications regardless of the manner in which they communicate. The Department has used the newly-amended pen/trap statute to track the communications of: (1) international terrorist conspirators, such as those in the Portland terror cell and the Virginia Jihad case; (2) domestic terrorists, such as an individual believed to be responsible for damaging electrical towers in Oregon and California; (3) major drug distributors; and (4) thieves who were able to obtain their victims' bank account information and loot the accounts. Section 216 has also proven extremely useful in other terrorism cases and in combating computer crime.

Examples:

- Section 216 was critical in disrupting a plot to use cocaine to purchase Soviet bloc weapons for the United Self Defense Forces of Colombia, which has been designated as a foreign terrorist organization by the State Department. Investigators used the authorities contained in section 216 of the USA PATRIOT Act to secure a pen/trap on targets of the investigation. The information obtained through the pen/traps, coupled with a wire intercept, then allowed investigators to secure a court order to intercept the communications of one of the targets. These intercepted communications, in turn, provided substantive evidence against several of the targets. As a result of this investigation, an indictment was returned against four defendants charging them with conspiring to provide material support to a foreign terrorist organization and conspiring to distribute five kilograms or more of cocaine. All four defendants have been arrested. Two defendants have pleaded guilty to both counts of the indictment, and one has pleaded guilty to the material support count. The final defendant, who was recently extradited from Costa Rica, is awaiting trial.

- Investigators recently used section 216 and other USA PATRIOT Act authorities to combat credit card fraud perpetrated over the Internet. In this case, customers of an Internet service provider were being target by "phishers." The phishers sent e-mail messages that appeared to be from the Internet service provider, asking the customer to click on a link to enter new or updated credit card information. Once the customer clicked on a link, he or she was sent to what appeared to be an official site of the Internet service provider but was really a website created by the phisher. Once the customers entered their credit card information, the website e-mailed the data to a web-based e-mail account. Phishers then used this information for their financial benefit, and the loss to the customers of the Internet service provider from this activity has been estimated in the millions.

  Because fraudulent e-mail accounts and websites go up and down quickly, the use of USA PATRIOT Act authorities by investigators was critical to the identification and prosecution of one of the phishers. Investigators used section 216 to obtain pen/traps for Internet service providers located in another state, used section 210 to issue subpoenas to Internet service providers, and used section 220 to obtain search warrants for e-mail content from out-of-district Internet service providers. These USA PATRIOT Act authorities allowed investigators both to apprehend the phishers and to identify retailers who had been defrauded. One defendant has already pleaded guilty to charges as a result of this investigation, which would never have been successfully brought without the authorities contained in the USA PATRIOT Act.

- Investigators in California successfully used section 216 in their investigation of a hacker group committing distributed denial-of-service attacks on Internet service providers. These attacks flooded the targeted sites with meaningless messages and effectively shut them down. Significantly, some of the computers compromised by this hacker group were on military networks. At the start of the investigation, limited information was available to investigators concerning the identities and locations of the members of the hacking group. Investigators learned, however, that the distributed denial-of-service attacks were being accomplished from a certain server. Investigators therefore applied for and obtained authorization to use pen/traps to track down members of the hacking group, one of whom was later arrested and charged with hacking into a military network. The pen/traps were critical in furthering the investigation because they allowed investigators to obtain important information on a real-time basis and before any records were destroyed as part of the service provider's routine business.

The USA PATRIOT Act also has updated federal pen/trap law under FISA by making the legal requirements for obtaining court permission for pen/trap orders in international terrorism investigations more similar to the standards that apply in ordinary criminal cases. Previously, FISA-authorized pen/trap orders were available in terrorism investigations only if the suspect

was, or was communicating with, an "agent of a foreign power."[5] FISA thus prevented officials from using pen/trap devices in many settings that might have revealed information relevant to a foreign intelligence investigation. Under section 214 of the Act, however, the government now can obtain a pen/trap order when the information likely to be obtained is foreign intelligence information or is relevant to investigations intended to protect against international terrorism or "clandestine intelligence activities." While specific examples of the use of pen/trap devices pursuant to section 214 remain classified, the Department has utilized section 214 on several occasions in international terrorism investigations, including investigations of suspected al Qaeda operatives in the United States, and the streamlined pen/trap authority has made it easier to identify additional subjects in terrorism investigations.

Section 201 of the USA PATRIOT Act brought the federal wiretap statute into the 21st century. Before the passage of the USA PATRIOT Act, law enforcement had the authority to conduct electronic surveillance – by petitioning a court for a wiretap order – when investigating many ordinary, non-terrorism crimes, such as drug crimes, mail fraud, and passport fraud, and some crimes that terrorists often commit. But wiretaps were not available to investigate other crimes likely to be committed by terrorists, such as chemical weapons offenses, killing United States nationals abroad, using weapons of mass destruction, and providing material support to terrorist organizations. Section 201 closed this gap by making wiretaps available in those investigations as well. Several recent wiretap orders have been based on this expanded list of terrorism offenses, including one involving a suspected domestic terrorist, who was subsequently charged with unlawfully making an explosive bomb, as well as another involving an individual with suspected ties to Columbian terrorists.

Cooperation of Third Parties

The cooperation of third parties in criminal or terrorist investigations is often crucial to a positive outcome. Third parties, such as telecommunications companies, often can assist law enforcement by providing information in emergency situations. Previous federal law, however, did not expressly allow telecommunications companies to disclose customer records or communications in emergencies. Even if a provider believed that it faced an emergency situation in which lives were at risk, if the provider turned over customer information to the government, it risked, in some circumstances, being sued for money damages. Congress remedied this problem in section 212 of the USA PATRIOT Act by allowing electronic communications service providers to disclose records to the government in situations involving an immediate danger of death or serious physical injury to any person. Section 212 has already amply proved its utility.

Examples:

- Section 212 was used in the investigation of a bomb threat against a school. An anonymous person, claiming to be a student at a high school, posted on the Internet a disturbing death threat singling out a faculty member and several

[5] 50 U.S.C. § 1801(b) (1978).

students to die by bomb and gun. The operator of the Internet site initially resisted disclosing to law enforcement any information about the suspect for fear that he could be sued if he volunteered that information. Once a prosecutor explained that the USA PATRIOT Act created a new provision allowing for the voluntary release of information in emergencies, the owner turned over evidence that led to the timely identification of the individual responsible for the bomb threat. Faced with this evidence, the suspect confessed to making the threats. The operator of the Internet site later revealed that he had been worried for the safety of the students and teachers for several days, and expressed his relief that the USA PATRIOT Act permitted him to help.

- Section 212 was recently used to apprehend quickly an individual threatening to destroy a Texas mosque before he could carry out his threat. Jared Bjarnason, a 30-year-old resident of El Paso, Texas, allegedly sent an e-mail message to the El Paso Islamic Center on April 18, 2004. In this message, he threatened to burn the Islamic Center's mosque to the ground if hostages in Iraq were not freed within three days. In their investigation of this threat, FBI agents utilized section 212 to obtain information quickly from electronic communications service providers leading to the identification and arrest of Bjarnason before he could harm the mosque. Absent section 212, however, it is not clear that investigators would have been able to locate and apprehend Bjarnason in time.

- Section 212 was invaluable in swiftly resolving a cyber-terrorist threat to the South Pole Research Station. Last year, the National Science Foundation (NSF) received an e-mail reading: "I've hacked into the server of your South Pole Research Station. Pay me off or I'll sell the station's data to another country and tell the world how vulnerable you are." The e-mail message further contained data only found on the NSF's computer systems, proving that the threat was real. The hacked computer also controlled the life support systems for the South Pole Station that housed 50 scientists "wintering over" during the South Pole's most dangerous season. At this time, aircraft could not land at the South Pole for another six months due to the harsh weather conditions. After receiving this e-mail message, investigators used section 212 of the USA PATRIOT Act to identify the hackers quickly. Due in part to the quick response allowed by section 212, FBI agents were able to close the case quickly with the suspects' arrest before any harm was done to the South Pole Research Station.

- Section 212 has further proven to be extremely useful in cases involving abducted or missing children. The provision, for instance, was instrumental in quickly rescuing a 13-year-old girl from Western Pennsylvania who had been lured from her home and was being held captive by a 38-year-old man she had met online. In early 2002, FBI agents received a report from the local police department that the girl had disappeared the previous day from her parents' home. The agents interviewed the parents and the girl's friends, one of whom reported that the girl had discussed leaving home with a man she had met online. In the next couple of

days, an anonymous caller contacted the FBI and stated that he had chatted online recently with an individual claiming to have taken a girl from Pittsburgh. Based on information provided by the anonymous caller, FBI agents in Pittsburgh quickly requested information from an Internet service provider pursuant to section 212. With the information provided in response to that request, agents were able to locate the perpetrator. They immediately went to his residence in Herndon, Virginia, and rescued the child victim. The suspect subsequently was arrested, pleaded guilty to charges of travel with intent to engage in sexual activity with a minor and sexual exploitation of a minor, and was sentenced to a prison term of over 19 years.

- Section 212 and other USA PATRIOT Act authorities were also critical to the safe recovery of an 88-year-old Wisconsin woman who was kidnapped and held for ransom in February 2003. Investigators swiftly used sections 210, 212, and 220 of the USA PATRIOT Act to gather information, including communications provided on an emergency basis from Internet service providers, that assisted in identifying several suspects and accomplices and then quickly locating the elderly victim. When the victim was found, she was bound in an unheated shed during a cold Wisconsin winter several feet from a suspect's residence. Thankfully, the victim fully recovered from her ordeal, which had lasted for several days. Without a doubt, the information obtained using section 212 and other provisions of the USA PATRIOT Act was instrumental in solving the case quickly and thus saving the victim's life. The suspect was eventually arrested and was prosecuted and convicted by Wisconsin authorities after it was determined the victim was not transported across state lines and thus could be more effectively prosecuted in state court.

The USA PATRIOT Act also empowered Internet service providers and others to enlist the help of law enforcement to monitor the activities of hackers who unlawfully access their computer networks. Section 217 of the Act allows victims of computer attacks by cyber-terrorists and others to ask law enforcement officers to monitor trespassers on their systems. Section 217 thus places cyber-intruders on the same footing as physical intruders: hacking victims can seek law-enforcement assistance to combat hackers just as burglary victims can invite police officers into their homes to catch burglars.

VI. Conclusion

As the Attorney General affirmed on November 8, 2001, the Department of Justice has been called to "the highest and most noble form of public service—the preservation of American lives and liberty."[6] Now, more than two years after the attacks of September 11, the Department continues to respond to this call with enthusiasm, and with a profound respect for this country's

[6] *See Attorney General Ashcroft and Deputy Attorney General Thompson Announce Reorganization and Mobilization of the Nation's Justice and Law Enforcement Resources*, November 8, 2001, *available at* http://www.usdoj.gov/ag/speeches/2001/agcrisisremarks11_08.htm.

tradition of civil rights and liberties. In prosecuting the war on terrorism, the Department has taken every appropriate step to prevent acts of terrorism and to protect innocent American lives. The Department also continues this campaign with a constant awareness of its obligation to preserve freedom and with scrupulous attention to the legal and constitutional protections for civil liberties.

The USA PATRIOT Act has played a vital role in the Department of Justice's efforts to preserve America's system of ordered liberty for future generations. Since the Act was passed over two years ago, the Department of Justice has deployed its new authorities urgently in an effort to incapacitate terrorists before they can launch another attack, and, as demonstrated by the examples contained in this report, the Act's successes already are evident. The USA PATRIOT Act has facilitated the prosecution of terrorists and their supporters across the nation. It has authorized law enforcement and intelligence officers to share information and coordinate with one another. It has provided intelligence and law enforcement officials with the tools they need to fight terrorism in a digital age. It has assisted in curtailing the flow of funds to terrorists and terrorist organizations. And it has helped the Department to combat serious criminal conduct, such as child abduction and child pornography. For all of these reasons, the USA PATRIOT Act has made Americans safer over the course of the past two-and-a-half years, and the Department of Justice fully expects that the Act will continue to enhance the security of the American people in the future.

671706

U.S. Department of Justice

Criminal Division

Assistant Attorney General *Washington, D.C. 20530*

October 1, 2004

MEMORANDUM

TO: William Moschella
Assistant Attorney General
Legislative Affairs

FROM: CAW Christopher A. Wray
by
Assistant Attorney General

SUBJECT: Pen Register/Trap and Trace Report to Congress

The provisions of the Electronic Communications Privacy Act of 1986, Public Law 99-508, codified at 18 U.S.C. 3126, provide that the Attorney General of the United States shall report to Congress on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice (DOJ).

The enclosed report, compiled from individual reports submitted by the Federal Bureau of Investigation; the Drug Enforcement Administration; the Immigration and Naturalization Service (during the period that it was a DOJ agency); the United States Marshals Service; and the Office of the Inspector General, reflects the activity of these agencies/offices in this area for calendar years 1999 through 2003 and are reported on behalf of the Attorney General. The specific reports of the five components are also enclosed. We have not yet been able to obtain a report from the Bureau of Alcohol, Tobacco, Firearms and Explosives (for the period that it has been a DOJ agency).

Please return the signed letters to the Office of Enforcement Operations (OEO) within the Criminal Division. If you have questions concerning the letters or enclosures, please contact Janet Webb, Principal Associate Director for Operations within OEO, at 4-6809.

Attachments

U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General
Washington, D.C. 20530

November 3, 2004

The Honorable Orrin G. Hatch
Chairman, Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

The provisions of the Electronic Communications Privacy Act of 1986, Public Law 99-508, codified at 18 U.S.C. 3126, provide that the Attorney General of the United States shall report to Congress on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice (DOJ).

The enclosed report, compiled from individual reports submitted by the Federal Bureau of Investigation; the Drug Enforcement Administration; the Immigration and Naturalization Service (during the period that it was a DOJ agency); the United States Marshals Service; the Bureau of Alcohol, Tobacco, Firearms and Explosives (for the period that it has been a DOJ agency); and the Office of the Inspector General, reflects the activity of these agencies/offices in this area for calendar years 1999 through 2003 and are reported on behalf of the Attorney General. The specific reports of the six components are also enclosed.

The report contains information on the number of original and extension applications for orders made to the courts for authorization to use both pen registers and trap and trace devices, information concerning the number of investigations involved, the offenses on which the applications were predicated, and the number of people whose telephone facilities were affected. Information on the offenses involved is set forth in the individual agency reports.

Sincerely,

William E. Moschella

William Moschella
Assistant Attorney General

Enclosures

U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

November 3, 2004

The Honorable Patrick J. Leahy
Ranking Minority Member
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Senator Leahy:

The provisions of the Electronic Communications Privacy Act of 1986, Public Law 99-508, codified at 18 U.S.C. 3126, provide that the Attorney General of the United States shall report to Congress on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice (DOJ).

The enclosed report, compiled from individual reports submitted by the Federal Bureau of Investigation; the Drug Enforcement Administration; the Immigration and Naturalization Service (during the period that it was a DOJ agency); the United States Marshals Service; the Bureau of Alcohol, Tobacco, Firearms and Explosives (for the period that it has been a DOJ agency); and the Office of the Inspector General, reflects the activity of these agencies/offices in this area for calendar years 1999 through 2003 and are reported on behalf of the Attorney General. The specific reports of the six components are also enclosed.

The report contains information on the number of original and extension applications for orders made to the courts for authorization to use both pen registers and trap and trace devices, information concerning the number of investigations involved, the offenses on which the applications were predicated, and the number of people whose telephone facilities were affected. Information on the offenses involved is set forth in the individual agency reports.

Sincerely,

William E. Moschella

William Moschella
Assistant Attorney General

Enclosures

U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

November 3, 2004

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

Dear Mr. Chairman:

The provisions of the Electronic Communications Privacy Act of 1986, Public Law 99-508, codified at 18 U.S.C. 3126, provide that the Attorney General of the United States shall report to Congress on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice (DOJ).

The enclosed report, compiled from individual reports submitted by the Federal Bureau of Investigation; the Drug Enforcement Administration; the Immigration and Naturalization Service (during the period that it was a DOJ agency); the United States Marshals Service; the Bureau of Alcohol, Tobacco, Firearms and Explosives (for the period that it has been a DOJ agency); and the Office of the Inspector General, reflects the activity of these agencies/offices in this area for calendar years 1999 through 2003 and are reported on behalf of the Attorney General. The specific reports of the six components are also enclosed.

The report contains information on the number of original and extension applications for orders made to the courts for authorization to use both pen registers and trap and trace devices, information concerning the number of investigations involved, the offenses on which the applications were predicated, and the number of people whose telephone facilities were affected. Information on the offenses involved is set forth in the individual agency reports.

Sincerely,

William E. Moschella

William Moschella
Assistant Attorney General

Enclosures

U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

November 3, 2004

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

Dear Congressman Conyers:

The provisions of the Electronic Communications Privacy Act of 1986, Public Law 99-508, codified at 18 U.S.C. 3126, provide that the Attorney General of the United States shall report to Congress on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice (DOJ).

The enclosed report, compiled from individual reports submitted by the Federal Bureau of Investigation; the Drug Enforcement Administration; the Immigration and Naturalization Service (during the period that it was a DOJ agency); the United States Marshals Service; the Bureau of Alcohol, Tobacco, Firearms and Explosives (for the period that it has been a DOJ agency); and the Office of the Inspector General, reflects the activity of these agencies/offices in this area for calendar years 1999 through 2003 and are reported on behalf of the Attorney General. The specific reports of the six components are also enclosed.

The report contains information on the number of original and extension applications for orders made to the courts for authorization to use both pen registers and trap and trace devices, information concerning the number of investigations involved, the offenses on which the applications were predicated, and the number of people whose telephone facilities were affected. Information on the offenses involved is set forth in the individual agency reports.

Sincerely,

William E. Moschella

William Moschella
Assistant Attorney General

Enclosures

Brand, Rachel

From: Berry, Matthew (OLP)
Sent: Monday, March 21, 2005 5:54 PM
To: Collins Cook, Beth; Brand, Rachel
Subject: RE: DAG QFR #23

[redacted]
Exemption (b)(5)

-----Original Message-----
From: Collins Cook, Beth
Sent: Monday, March 21, 2005 5:42 PM
To: Brand, Rachel
Cc: Berry, Matthew (OLP)
Subject: RE: DAG QFR #23

Here is a proposed answer. [redacted]
Exemption (b)(5)
[redacted]
Exemption (b)(5)

-----Original Message-----
From: Brand, Rachel
Sent: Friday, March 18, 2005 7:28 PM
To: Collins Cook, Beth
Cc: Berry, Matthew (OLP)
Subject: FW: DAG QFR #23

Beth, can you take a crack at this. [redacted]
Exemption (b)(5)

-----Original Message-----
From: Wade, Jill C
Sent: Tuesday, March 15, 2005 6:15 PM
To: Brand, Rachel
Subject: DAG QFR #23

Rachel:

23

Thanks for attending out PATRIOT reauth meeting this morning. We appreciated your input and I hope you found the meeting helpful.

For your reference, I have attached to this e-mail our April QFRs from the DAG's SJC Utah field hearing, as well as the latest version of our DAG SAFE Act QFRs, the latter of which will go to OMB this week.

[redacted] Exemption (b)(5)

#23: **There was an interesting article published by a law librarian in the Law Library Journal this summer entitled "Post-USA Patriot Act Electronic Surveillance at the Library." The author explains how law enforcement can now watch what library patrons are reading online, while they are reading it, with a simple pen register order obtained under Section 216 of the PATRIOT Act. This is because, and I'm quoting from the author here, "by simply conflating email headers and web site addresses with telephone numbers, and conflating a particular technology for telephones with the full range of computer interception devices (including the FBI's Carnivore program), the potential range of information retrievable has been exponentially increased."**

Is it true that post-PATRIOT Act, a pen register attached to a library computer can easily recover information such as web sites visited, pages downloaded, online order forms accessed, and pictures viewed, rather than just simple numbers "called" by the computer? If so, would you agree that it raises heightened Fourth Amendment concerns and the need to treat this information differently?

[redacted] Exemption (b)(5)

#24 **On May 24, 2002, your predecessor issued a memorandum to field offices instructing them on how to prevent "overcollection" -- i.e., the inadvertent gathering of communication content -- when using pen/trap devices. How has your office exercised oversight on this directive? Have there been overcollections of content and were they ever used in cases or investigations?**

ANSWER: [redacted] Exemption (b)(5)

#25 **The U.S. Attorney's Manual addresses the May 24 memo. One issue that has been raised in this regard is whether a pen register order may be used to collect the URLs (the address of a page on the World Wide Web). Because of privacy and other concerns relating to the use of pen register orders in this fashion, prosecutors are required to have prior consultation with the Department in order to collect all or part of a URL with a pen register order. Can you bring me up to date on this issue -- have there been consultations and subsequent approvals and on what basis and in what circumstances?**

ANSWER: [redacted] Exemption (b)(5)

<< File: 02-07-05 Ltr re Comey QFRs from 04-14-04 hearing re Preventing and Responding to Acts of Terrorism.pdf >> << File: DAG-QFRS-092204-COMP-021605.doc >>

Please let me know if I can provide any additional information.
Thank you,

~J~

Jill C. Wade
Office of Legislative Affairs
U.S. DEPARTMENT OF JUSTICE
(202) 514-2141 (phone)
(202) 305-2643 (fax)
Jill.C.Wade@USDOJ.gov