

EXHIBIT “AA”

[Residential](#)[Small Business](#)[Medium Business](#)[Large Business](#)[Wireless](#)[News Center Main Page](#)[News Archive](#)[Media Contacts](#)[Press Kits](#)[Executive Center](#)[Video & Image Feed](#)

News Release

Verizon Issues Statement on NSA and Privacy Protection

May 12, 2006

Media Contact:

[Peter Thonis](#), 212-395-2355

NEW YORK -- *Verizon Communications Inc. (NYSE:VZ) today issued the following statement:*

The President has referred to an NSA program, which he authorized, directed against al-Qaeda. Because that program is highly classified, Verizon cannot comment on that program, nor can we confirm or deny whether we have had any relationship to it.

Having said that, there have been factual errors in press coverage about the way Verizon handles customer information in general. Verizon puts the interests of our customers first and has a longstanding commitment to vigorously safeguard our customers' privacy -- a commitment we've highlighted in our privacy principles, which are available at www.verizon.com/privacy.

Verizon will provide customer information to a government agency only where authorized by law for appropriately-defined and focused purposes. When information is provided, Verizon seeks to ensure it is properly used for that purpose and is subject to appropriate safeguards against improper use. Verizon does not, and will not, provide any government agency unfettered access to our customer records or provide information to the government under circumstances that would allow a fishing expedition.

In January 2006, Verizon acquired MCI, and we are ensuring that Verizon's policies are implemented at that entity and that all its activities fully comply with law.

Verizon hopes that the Administration and the Congress can come together and agree on a process in an appropriate setting, and with safeguards for protecting classified information, to examine any issues that have been raised about the program. Verizon is fully prepared to participate in such a process.

####

Regis
news
e-mail

[RSS](#)
[Click I](#)
availa
Verizc
[XML](#)

[En es](#)
[Click I](#)
News
Spani

EXHIBIT “BB”



Residential

Small Business

Medium Business

Large Business

Wireless

[News Center Main Page](#)

[News Archive](#)

[Media Contacts](#)

[Press Kits](#)

[Executive Center](#)

[Video & Image Feed](#)

News Release

Verizon Issues Statement on NSA Media Coverage

May 16, 2006

Media Contact:

[Peter Thonis](#), 212-395-2355

NEW YORK -- *Verizon Communications Inc. (NYSE:VZ) today issued the following statement regarding news coverage about the NSA program which the President has acknowledged authorizing against al-Qaeda:*

As the President has made clear, the NSA program he acknowledged authorizing against al-Qaeda is highly-classified. Verizon cannot and will not comment on the program. Verizon cannot and will not confirm or deny whether it has any relationship to it.

That said, media reports made claims about Verizon that are simply false.

One of the most glaring and repeated falsehoods in the media reporting is the assertion that, in the aftermath of the 9/11 attacks, Verizon was approached by NSA and entered into an arrangement to provide the NSA with data from its customers' domestic calls.

This is false. From the time of the 9/11 attacks until just four months ago, Verizon had three major businesses - its wireline phone business, its wireless company and its directory publishing business. It also had its own Internet Service Provider and long-distance businesses. Contrary to the media reports, Verizon was not asked by NSA to provide, nor did Verizon provide, customer phone records from any of these businesses, or any call data from those records. None of these companies - wireless or wireline - provided customer records or call data.

Another error is the claim that data on local calls is being turned over to NSA and that simple "calls across town" are being "tracked." In fact, phone companies do not even make records of local calls in most cases because the vast majority of customers are not billed per call for local calls. In any event, the claim is just wrong. As stated above, Verizon's wireless and wireline companies did not provide to NSA customer records or call data, local or otherwise.

Again, Verizon cannot and will not confirm or deny whether it has any relationship to the classified NSA program. Verizon always stands ready, however, to help protect the country from terrorist attack. We owe this duty to our fellow citizens. We also have a duty, that we have always fulfilled, to protect the privacy of our customers. The two are not in conflict. When asked for help, we will always make sure that any assistance is authorized by law and that our customers' privacy is safeguarded.

####

Regis
news
e-mail

[RSS](#)
[Click I](#)
availa
Verizc
[XML](#)

[En es](#)
[Click I](#)
News
Spani

EXHIBIT “CC”

EARN UP TO 3 FREE NIGHTS WITH 1ST PURCHASE.

THE STARWOOD PREFERRED GUEST® CREDIT CARD FROM AMERICAN EXPRESS



> APPLY NOW

FIRST YEAR FEE-FREE.



Powered by

Verizon says it isn't giving call records to NSA

Updated 5/16/2006 11:43 PM ET

By Jim Drinkard, USA TODAY

Verizon said in a statement Tuesday that it is not providing customer calling information to the National Security Agency.

"One of the most glaring and repeated falsehoods in the media reporting," the statement said, "is the assertion that, in the aftermath of the 9/11 attacks, Verizon was approached by NSA and entered into an arrangement to provide the NSA with data from its customers' domestic calls. This is false."

Last Thursday, USA TODAY reported that the NSA has been secretly collecting the phone call records of tens of millions of Americans, using data provided by AT&T, BellSouth and Verizon, citing people with direct knowledge of the program.

Long-distance calls placed by BellSouth and Verizon subscribers can traverse the networks of other carriers who collect a variety of information for billing purposes. Verizon's statement leaves open the possibility that the NSA directed its requests to long-distance companies, or that call data was collected by means other than Verizon handing them over, the Associated Press reported Tuesday.

On Monday, BellSouth denied providing records to the NSA. AT&T has refused to confirm or deny that it gave records to the NSA. One of the nation's major telecommunication companies, Qwest, declined to participate in the NSA program, the story said, a fact confirmed Friday by Herbert Stern, the lawyer for former Qwest CEO Joe Nacchio.

For the initial story, Verizon issued a statement saying, "We do not comment on national security matters, we act in full compliance with the law and we are committed to safeguarding our customers' privacy."

Since then, the three companies named in the story have been named in a lawsuit seeking \$200 billion in damages. The lawsuit filed in U.S. District Court in Manhattan claims the companies violated telecommunications law and the Constitution by allowing the government to have call information.

In response to the Verizon statement, Steve Anderson, USA TODAY's director of communications, said: "We will continue to investigate and pursue the story. We're confident in our coverage of the phone database story. We will look closely into the issues raised by the BellSouth and Verizon statements."

Advertisement

A vertical advertisement for Verizon Wireless. At the top is the Verizon Wireless logo. Below it, the text "Get The LG Phone That Fits You Best" is displayed in a large, bold, sans-serif font. At the bottom, there is a photograph of a silver LG phone with a red Verizon checkmark on its screen.

Verizon's statement does not mention MCI, the long-distance carrier the company bought in January. Before the sale, Verizon sold long-distance under its own brand. Asked to elaborate on what role MCI had, or is having, in the NSA program, spokesman Peter Thonis said the statement was about Verizon, not MCI.

Asked whether Verizon's customer calling records are in the NSA database, Thonis said, "I just don't know the answer to that."

On whether BellSouth's customer records are in the National Security Agency's database, Jeff Battcher, a company spokesman, said: "We're not aware of any database that NSA has, so we're not aware of our customer information being there at all."

The third company, AT&T, said last week that it would help government efforts only within the limits of the law. On Tuesday, company spokesman Michael Coe said AT&T had no additional comment.

Asked about the denials, Sen. Patrick Leahy of Vermont, the senior Democrat on the Senate Judiciary Committee, noted that telephone company executives will be called before the panel for a hearing. "We'll ask them under oath," he said.

"The thing that concerns me is some (companies) said yes and some said no" when asked to participate. "If the government really thought this was legal and necessary, why let some say yes and some say no? It's either legal and necessary, or it's not."

At the White House, President Bush renewed his defense of telephone surveillance in answer to a question about whether Americans might feel that their privacy is being invaded.

BUSH:[Surveillance legal](#)

The government's effort is to "connect dots to protect the American people, within the law," he said. "The program ... is one that has been fully briefed to members of the United States Congress, in both political parties."

Afterward, White House press secretary Tony Snow denied that Bush's answer amounted to a confirmation of the reported database project. "He was not giving a back-handed confirmation," Snow said. "But I would direct you back to the USA TODAY story itself. It said there is no wiretapping of individual calls, there is no personal information that is being relayed."

At the same time, the chairmen of the House and Senate intelligence committees announced that all members of the two panels would receive briefings on the NSA's Terrorist Surveillance Program.

Bush's nominee to head the Central Intelligence Agency, Air Force Gen. Michael Hayden, is scheduled to go before the Senate panel for a confirmation hearing on Thursday. Hayden headed the NSA when the program was conceived and implemented after the Sept. 11, 2001, terrorist attacks.

"It became apparent that all members of my committee needed to know the full width and breadth of the president's program" said Senate Intelligence Committee Chairman Pat Roberts, R-Kan. "This issue will be central to the committee's deliberations on Gen. Hayden's nomination."

Contributing: Leslie Cauley in New York; John Diamond and Kathy Kiely in Washington; wire reports

Find this article at:

http://www.usatoday.com/news/washington/2006-05-16-verizon-nsa_x.htm

☐ Check the box to include the list of links referenced in the article.

Copyright 2007 USA TODAY, a division of Gannett Co. Inc.

.

EXHIBIT “DD”

2 of 7 DOCUMENTS

Copyright 2005 The New York Times Company
The New York Times

February 14, 2005 Monday
Late Edition - Final

SECTION: Section A; Column 1; National Desk; Pg. 1

LENGTH: 941 words

HEADLINE: Verizon Agrees to Acquire MCI For \$6.6 Billion, Beating Qwest

BYLINE: By MATT RICHTEL and ANDREW ROSS SORKIN

BODY:

Verizon, the nation's largest regional phone company, reached a deal last night to acquire MCI for about \$6.6 billion in cash and stock, the latest merger in the rapidly consolidating telecommunications industry.

The deal, which was approved by the boards of both companies late last night, is expected to be announced today, the executives close to the negotiations said.

Verizon's acquisition would end the independence of MCI, the nation's second-largest long-distance company, with 14 million residential customers and about a million corporate customers.

Last year MCI emerged from bankruptcy protection and changed its name from WorldCom after nearly collapsing when an \$11 billion accounting fraud was unearthed. MCI is a shadow of its former self, but its high-margin corporate customers and worldwide telephone and data network make it quite valuable.

MCI became the subject of a torrent of takeover interest among its rivals in recent weeks after SBC, the second-largest regional phone company in the nation, agreed to acquire AT&T for \$15 billion.

That left MCI one of the last remaining major telecommunications companies up for grabs. Indeed, Verizon defeated its much smaller rival, Qwest Communications, in an 11th hour takeover skirmish over the weekend for control of MCI.

Qwest had submitted several ever-increasing bids for MCI over the past week, the executives said. Late Friday night, Qwest submitted a final bid worth \$7.3 billion, the executives said. Still, MCI's board chose to accept Verizon's lower bid because it had concerns about Qwest's ability to finance the transaction and about the long-term value of Qwest's stock, the executives said.

The deal reflects Verizon's interest in growing its present business of selling telephone and data services to corporate customers, an operation said by industry analysts to be worth about \$250 billion a year. Still, the lure of MCI was considered more complicated than the acquisition of AT&T, in part because of the stigma of its recent bankruptcy.

Spokesmen for Verizon, MCI and Qwest all declined to comment. Mergers in the telecommunications industry have revived in the last few months after several years of declining sales, bankruptcies and accounting scandals.

Verizon Agrees to Acquire MCI For \$6.6 Billion, Beating Qwest The New York Times February 14, 2005 Monday

In December, Sprint and Nextel agreed to merge to form the third-largest wireless company. Less than a month later, Alltel, a regional cellular provider, said it would buy Western Wireless.

These deals, plus the one by SBC and AT&T, analysts said, were partly a response to the re-election of President Bush, whose administration has imposed relatively few restrictions on the merging of companies. While Verizon's agreement to acquire MCI will face regulatory scrutiny, legal experts have suggested the deal will probably be approved.

The lawyers said the antitrust analysis might be slightly more complicated because the deal is likely to be examined not just on its own but within the context of the entire industry, which is quickly being redrawn.

The acquisition of MCI reflects a marked and swift change sweeping the telecommunications industry, brought largely by shifts in technology. A combination of forces, like heavy reliance on wireless communications and the Internet, have cut deeply into the traditional wired telephone business, forcing companies like Verizon to find new sources of revenue.

Even as the industry has evolved, it has in some ways gone backwards. A series of mergers in recent months has consolidated market power in the hands of a few companies. These companies, once the progeny of the breakup of AT&T, now are coming together again to form large regional telecommunications juggernauts, challenged only by an emerging cable industry.

For Verizon, MCI could be considered the consolation prize for not buying AT&T. But for MCI and Michael D. Capellas, who was brought in as chief executive to take the company out of bankruptcy and turn it around, the deal is a boon.

Industry analysts give Mr. Capellas high marks for cutting costs. He also began an aggressive sales effort to keep the company's biggest customers while it was operating under bankruptcy protection, which it exited in April last year with less debt relative to AT&T and \$5.6 billion in cash on its balance sheet.

But Mr. Capellas will not have a role at Verizon once the deal is completed, the executives said. Mr. Capellas was formerly the chief executive of Compaq Computers before selling it in 2002 to Hewlett-Packard.

Industry experts say MCI operationally is less impressive than AT&T. The company's share of the corporate phone and data market is roughly half of AT&T's, and it is considered by industry analysts to be less efficient than AT&T.

Michael Rollins, an analyst at Smith Barney, said each MCI employee generated \$425,000 in annual revenue, nearly 30 percent less than an AT&T worker. Its profit margins after deducting access charges paid to the Bells and others are 8 percentage points lower than AT&T's. The company also invests less on its network and operations.

UBS data show MCI having pretax profits in its two other major business sectors: one with customers ranging from midsize businesses down to consumers, which had \$9.1 billion in revenue in 2004; and another, with international corporate customers and wholesale network sales, or sales to other carriers, which hit \$6.6 billion in 2004.

MCI plans to report its fourth-quarter and full-year results in the next two weeks, but has yet to set a firm date. MCI shares were at \$20.80 during after-hours trading on Friday, up 34 cents from the close on Thursday; Verizon shares closed at \$36.31, a gain of 27 cents.

URL: <http://www.nytimes.com>

LOAD-DATE: February 14, 2005

EXHIBIT “EE”



NEWS

Federal Communications Commission
445 12th Street, S.W.
Washington, D. C. 20554

This is an unofficial announcement of Commission action. Release of the full text of a Commission order constitutes official action. See MCI v. FCC, 515 F.2d 385 (D.C. Circ 1974).

News media Information 202 / 418-0500
TTY 202 / 418-2555
Fax-On-Demand 202 / 418-2830
Internet: <http://www.fcc.gov>
<ftp.fcc.gov>

FOR IMMEDIATE RELEASE:
June 21, 2005

NEWS MEDIA CONTACT:
Mark Wigfield 202-418-0253
Email: Mark.Wigfield@fcc.gov

FEDERAL COMMUNICATIONS COMMISSION RELEASES **STUDY ON TELEPHONE TRENDS**

Washington D.C. – Today, the Federal Communications Commission (FCC) released its *Trends in Telephone Service* report, which summarizes in one convenient reference source information published in various reports over the course of the past year. The report provides answers to some of the most frequently asked questions about the telephone industry coming from consumers, members of Congress, other government agencies, telecommunications carriers, and members of the business and academic communities.

The report is available for reference in the FCC's Reference Information Center, Courtyard Level, 445 12th Street, S.W., Washington, D.C. 20554. Copies may be purchased by contacting Best Copy and Printing, Inc., Portals II, 445 12th Street S.W., Room CY-B402, Washington, D.C. 20554, telephone 800-378-3160, facsimile 202-488-5563, or via e-mail at fcc@bcpiweb.com. This report can be downloaded from the **FCC-State Link** Internet site at:
www.fcc.gov/wcb/iatd/trends.html.

- FCC -

For additional information, contact Katie Rangos of the Wireline Competition Bureau's Industry Analysis and Technology Division, (202) 418-0940, or for users of TTY equipment, call (202) 418-0484.

Trends in Telephone Service

***Industry Analysis and Technology Division
Wireline Competition Bureau***

***Tables Compiled as of
April 2005***

This report is available for reference in the FCC's Information Center at 445 12th Street, S.W., Courtyard Level. Copies may be purchased by calling Best Copy and Printing, Inc., Portals II, 445 12th Street S.W., Room CY-B402, Washington DC 20554 at 800-378-3160, facimile 202-488-5563, or via e-mail fcc@bcpiweb.com. The report can also be downloaded from the **FCC-State Link** Internet site at: www.fcc.gov/wcb/trends.html.

Table of Contents

Introduction	1-1
Access Charges	1-1
Table 1.1 Interstate Per-Line Access Charges	1-3
Table 1.2 Interstate Per-Minute Access Charges.....	1-4
Table 1.3 Interstate Per-Line Access Charges by Carrier.....	1-5
Table 1.4 Interstate Per-Minute Access Charges by Carrier	1-6
Advanced Telecommunications	2-1
Table 2.1 High-Speed Lines	2-3
Chart 2.1 Total High-Speed Lines	2-3
Chart 2.2 High-Speed Lines by Technology	2-3
Table 2.2 Advanced Services Lines.....	2-4
Chart 2.3 Advanced Services Lines.....	2-4
Chart 2.4 Advanced Services Lines by Technology.....	2-4
Table 2.3 Residential and Small Business High-Speed Lines	2-5
Chart 2.5 Residential and Small Business High-Speed Lines	2-5
Chart 2.6 Residential and Small Business High-Speed Lines by Technology	2-5
Table 2.4 Residential and Small Business Advanced Services Lines	2-6
Chart 2.7 Residential and Small Business Advanced Services Lines.....	2-6
Chart 2.8 Residential and Small Business Advanced Services Lines by Technology	2-6
Table 2.5 High-Speed Lines by Technology as of June 30, 2004	2-8
Table 2.6 High-Speed Lines by State	2-9
Chart 2.9 Percent of U.S. Households with Computers, Internet Access, And High-Speed Access	2-10
Table 2.7 Percent of U.S. Households with Internet and High-Speed Access: Rural versus Urban	2-11
Chart 2.10 Percent of U.S. Households with Internet and High-Speed Access: Rural versus Urban	2-11
Consumer Expenditures	3-1
Table 3.1 Household Expenditures for Telephone Service	3-3
Table 3.2 Average Monthly Household Telecommunications Expenditures By Type of Provider.....	3-4
Earnings	4-1
Table 4.1 Interstate Rate-of-Return Summary Years 1997 through 2003	4-3
Employment and Labor Productivity	5-1
Table 5.1 Annual Average Number of Employees in the Telecommunications Industry	5-3
Chart 5.1 Annual Average Number of Employees in the Telecommunications Industry	5-3
Table 5.2 Labor Productivity Index for the Wired and Wireless	

Telecommunications Industry Measured in Output per Hour (OPH).....	5-4
Chart 5.2 Wired and Wireless Telecommunications Carriers (NAICS 5171 and 5172) Labor Productivity Index.....	5-4
Table 5.3 Number of Telecommunications Service Providers by Size of Business.....	5-5
International Telephone Service.....	6-1
Table 6.1 International Service from the United States.....	6-3
Chart 6.1 Billed Revenues per Minute and per Call	6-3
Table 6.2 International Telephone Service Settlements	6-4
Table 6.3 International Message Telephone Service for 2003	6-5
Chart 6.2 U.S. Billed Minutes by Country	6-5
Table 6.4 U.S. Billed Revenues of Facilities-Based and Facilities-Resale Carriers In 2003	6-6
Table 6.5 Top Providers of Pure Resale International MTS in 2003	6-7
Lines	7-1
Table 7.1 U.S. Wireline Telephone Lines	7-3
Table 7.2 Telephone Loops of Incumbent Local Exchange Carriers by State	7-4
Table 7.3 Telephone Loops of Incumbent Local Exchange Carriers by Holding Company.....	7-5
Chart 7.1 Five Largest Holding Companies' Share of Loops.....	7-5
Table 7.4 Additional Residential Lines for Households with Telephone Service.....	7-6
Table 7.5 Number of Payphones Owned by LECs and Independent Operators.....	7-7
Table 7.6 Number of Payphones Over Time	7-8
Local Telephone Competition.....	8-1
Table 8.1 End-User Switched Access Lines Reported	8-5
Chart 8.1 End-User Switched Access Lines Reported	8-5
Table 8.2 End-User Switched Access Lines by Customer Type	8-6
Chart 8.2 Percent of Lines that Serve Residential and Small Business Customers.....	8-6
Table 8.3 Reporting Competitive Local Exchange Carriers.....	8-7
Chart 8.3 Competitive Local Exchange Carriers' End-User Lines	8-7
Table 8.4 Reporting Incumbent Local Exchange Carriers	8-8
Chart 8.4 ILEC Lines and the Percent Provided to Other Carriers.....	8-8
Table 8.5 End-User Switched Access Lines Served By Reporting Local Exchange Carriers	8-9
Table 8.6 Competitive Local Exchange Carrier Share Of End-User Switched Access Lines.....	8-10
Table 8.7 Nationwide Local Service Revenues and New Competitors' Share	8-11
Chart 8.5 ILEC and New Local Competitor Share of Local Service Revenues	8-11
Table 8.8 Telephone Numbers in the Porting Database at the End of Each Quarter.....	8-13
Table 8.9 Telephone Numbers in the Porting Database as of December 31, 2004	8-14
Table 8.10 Telephone Number Porting Activity Since Wireless Pooling Started.....	8-15
Long Distance Telephone Industry	9-1
Table 9.1 Total Toll Service Revenues by Provider	9-5
Table 9.2 Intrastate, Interstate, and International Toll Revenues	9-7

Table 9.3	End-User Toll Revenues	9-8
Table 9.4	Number of Toll Service Providers	9-9
Table 9.5	Toll Revenues of AT&T, MCI, Sprint and Other Toll Service Providers.....	9-10
Table 9.6	Shares of Total Toll Service Revenues – All Long Distance Toll Providers	9-11
Chart 9.2	Market Shares of Toll Service Revenues of the Three Largest Long Distance Toll Providers Including ILECs, CLECs, and Wireless Carriers	9-11
Table 9.7	Residential Household Market Shares.....	9-12
Chart 9.3	Residential Household Market Shares	9-12
Table 9.8	Residential Household Market Shares by Region: 2003	9-14
Chart 9.4	Residential Household Market Shares by Region: 2003	9-14
Table 9.9	Regional Bell Operating Companies’ Applications To Provide In-Region InterLATA Service	9-16
Minutes.....		10-1
Table 10.1	Interstate Switched Access Minutes	10-3
Chart 10.1	Interstate Switched Access Minutes	10-3
Table 10.2	Telephone Calls and Billed Access Minutes of Large ILECs Reporting to the Commission	10-4
Mobile Wireless Service.....		11-1
Table 11.1	Measures of Mobile Wireless Telephone Subscribers.....	11-3
Chart 11.1	Mobile Wireless Telephone Subscribers	11-4
Table 11.2	Mobile Wireless Telephone Subscribers	11-5
Table 11.3	Mobile Wireless Telephone Service: Industry Survey Results	11-6
Table 11.4	Distribution of Residential Wireless Calls and Minutes	11-7
Table 11.5	Duration of Residential Wireless Calls: 2003	11-8
Table 11.6	Distribution of Residential Intrastate Wireless Minutes by Day and Time.....	11-9
Table 11.7	Distribution of Residential Interstate Wireless Minutes by Day and Time.....	11-10
Price Indices for Telephone Services.....		12-1
Table 12.1	Long-Term Changes for Various Price Indices	12-3
Chart 12.1	CPI All Items and CPI Telephone Services	12-3
Table 12.2	Annual Changes in Major Price Indices	12-4
Chart 12.2	Percentage Change in CPI All Items and CPI Telephone Services	12-4
Table 12.3	Annual Changes in Price Indices for Local and Long Distance Telephone Services	12-5
Chart 12.3	CPI Telephone Service Price Indices.....	12-5
Price Levels		13-1
Table 13.1	Average Residential Rates for Local Service in Urban Areas, 1986 - 2004	13-3
Table 13.2	Average Local Rates for Businesses with a Single Line In Urban Areas, 1989 - 2004	13-4
Table 13.3	Average Rate for a Residential Access Line	13-5
Table 13.4	Average Revenue per Minute	13-6
Chart 13.1	Revenue per Minute for Interstate Calls	13-7

Residential Wireline Usage 14-1

Table 14.1	Distribution of Residential Wireline Toll Calls and Minutes	14-3
Table 14.2	Average Residential Wireline Monthly Toll Minutes	14-3
Table 14.3	Distribution of Residential Wireline Long Distance Call Durations: 2003.....	14-4
Table 14.4	Duration and Distance of Intrastate Toll Calls	14-5
Table 14.5	Duration and Distance of Interstate Toll Calls	14-5
Table 14.6	Distribution of Residential Wireline Long Distance Minutes By Day and Time	14-6

Revenues..... 15-1

Table 15.1	Telecommunications Industry Revenues	15-3
Chart 15.1	End-User Telecommunications Revenues	15-3
Table 15.2	Telecommunications Revenues Reported by Type of Service	15-4
Table 15.3	Number of Interstate Telecommunications Providers By Principal Type of Business.....	15-5
Table 15.4	Gross Revenues Reported by Type of Carrier	15-6
Table 15.5	Total Telecommunications Revenues by State.....	15-7
Table 15.6	Telecommunications Revenues by State: 2003	15-8
Table 15.7	Telecommunications Revenues by Type of Service: 2003.....	15-9

Subscribership 16-1

Table 16.1	Household Telephone Subscribership in the United States	16-3
Table 16.2	Telephone Penetration by State	16-4
Table 16.3	Telephone Subscribership on American Indian Reservations And Off-Reservation Trust Lands: Federal	16-5
Table 16.4	Historical Telephone Penetration Estimates.....	16-6
Table 16.5	Percentage of Households with Wireline and Cellular Service By Rural and Non-Rural Demographics.....	16-6

Technology Development 17-1

Table 17.1	Central Offices and Access Lines by Technology.....	17-5
Table 17.2	Features Available in Central Offices.....	17-6
Table 17.3	Switches by Metropolitan Statistical Area (MSA) And Non-MSA and Switches by Line Counts.....	17-7
Table 17.4	Local Transmission Technology.....	17-8
Table 17.5	Central Offices Converted to Equal Access	17-9
Table 17.6	Status of Selected Network Capabilities of 2003 Access Market Survey Respondents: Selected Rural ILECs.....	17-10
Chart 17.1	Telecommunications Patents	17-11
Table 17.7	Capital Expenditures for Structures and Equipment	17-12
Chart 17.2	Capital Expenditures for Structures and Equipment by Carrier	17-13

Telephone Numbers 18-1

Table 18.1	Area Codes by State.....	18-3
Table 18.2	Area Code Assignments.....	18-4

Table 18.3 Telephone Numbers Assigned for Toll-Free Service (800, 888, 877, 866)	18-6
Chart 18.1 Working Toll-Free Numbers.....	18-6
Table 18.4 Telephone Numbers Assigned for 800 Toll-Free Service	18-7
Table 18.5 Telephone Numbers Assigned for 888 Toll-Free Service	18-8
Table 18.6 Telephone Numbers Assigned for 877 Toll-Free Service	18-9
Table 18.7 Telephone Numbers Assigned for 866 Toll-Free Service	18-10
Table 18.8 Dialing Patterns of the United States.....	18-11
Universal Service.....	19-1
Table 19.1 Universal Service Support Mechanisms.....	19-5
Chart 19.1 Distribution of Universal Service Payments.....	19-5
Table 19.2 Universal Service Support Received by Service Provider Type: 2004	19-6
Chart 19.2 Universal Service Support Received by Service Provider Type	19-6
Table 19.3 High-Cost Support Payment History	19-7
Chart 19.3 Total High-Cost Support Fund Payment.....	19-7
Table 19.4 High-Cost Support Payments by State: 2004	19-8
Table 19.5 High-Cost Support Received by ILECs and CETCs	19-9
Chart 19.4 Percent of High-Cost Support Received by CETCs	19-9
Table 19.6 High-Cost Support by Type of Carriers: 2004	19-10
Table 19.7 Lifeline Monthly Support by State or Jurisdiction	19-11
Table 19.8 Lifeline Subscribers and Link-Up Beneficiaries	19-12
Table 19.9 Lifeline Subscribers and Link-Up Beneficiaries By State or Jurisdictions	19-13
Table 19.10 Low-Income Support Payments.....	19-15
Chart 19.5 Lifeline and Link-Up Support Payments	19-15
Table 19.11 Low-Income Support Payments by State or Jurisdiction: 2004	19-16
Table 19.12 Schools and Libraries Funding by Type of Service.....	19-17
Chart 19.6 Total Schools and Libraries Funds Committed and Disbursed	19-17
Table 19.13 Schools and Libraries Funding by State and by Type of Service.....	19-18
Table 19.14 Rural Health Care Fund Disbursements by Service Speed	19-19
Chart 19.7 Rural Health Care Fund Disbursements by Service Speed.....	19-19
Table 19.15 Rural Health Care Fund Disbursements by Service Speed and by State.....	19-20
Table 19.16 Universal Service Fund Contribution Factors	19-21
Table 19.17 Share of Universal Service Fund Contributions By Principal Type of Contributor Using Traditional Carrier Categories	19-22
Chart 19.8 Share of Universal Service Fund Contributions By Principal Type of Contributor	19-22
Appendix A – List of Publications by the Industry Analysis and Technology Division.....	20-A
Appendix B – Sources of Telecommunications Information	21-A
Appendix C – Contacting the Report Authors.....	22-A

Table 9.6
Shares of Total Toll Service Revenues
All Long Distance Toll Providers *

Year	AT&T	MCI	Sprint	BellSouth ¹	Qwest ¹	SBC ¹	Verizon ¹	Other Incumbent Local Telephone Companies	All Other Toll Service Providers ²
				Includes Incumbent Local Exchange Carriers' Operating Companies					
1984	68.3 %	3.4 %	2.1 %					24.2 %	2.0 %
1985	67.1	4.3	2.0					22.2	4.4
1986	63.5	5.9	3.3					22.4	4.9
1987	60.2	6.7	4.4					23.5	5.2
1988	56.6	7.8	5.4					24.1	6.1
1989	52.3	9.5	6.5					22.5	9.1
1990	50.7	11.3	7.5					22.0	8.4
1991	50.2	12.5	7.8					20.6	9.0
1992	47.3	13.9	7.5					17.9	13.4
1993	43.7	14.7	7.4					16.6	17.6
1994	44.4	16.5	8.1					15.9	15.2
1995	42.8	20.4	8.1					12.6	16.0
1996	39.4	20.9	8.0					11.3	20.4
1997	39.2	22.9	8.5					10.2	19.3
1998	38.6	21.1	7.6					9.0	23.7
1999	36.9	21.7	9.0					7.4	25.0
2000	34.8	20.6	8.3	0.4 %	3.1 %	2.7 %	3.1 %	NA	27.1
2001	34.2	21.4	8.5	0.7	3.5	3.1	3.4	NA	25.3
2002	32.9	21.1	8.5	1.0	4.0	3.7	3.7	NA	25.1
2003	30.0	20.8	8.2	1.6 p	3.8	4.9	5.2	NA	25.8

NA - Not applicable

* Includes incumbent local exchange carriers and competitive local exchange carriers.

¹ Figures reported by RBOC long distance affiliates, which may include both in-region and out-of-region long distance service, and local exchange operating companies for the years 2000 - 2003. Some of the RBOC long distance affiliates' revenues fall below the reporting threshold and are therefore included in the all other long distance carriers' market share.

² Includes wireless toll service revenues reported by wireless carriers and toll service revenues reported by competitive local exchange carriers. For 2000 - 2003, also includes non-RBOC ILEC toll service revenues.

Chart 9.2
Market Shares of Toll Service Revenues of the Three Largest Long Distance Toll Providers Including ILECs, CLECs, and Wireless Carriers

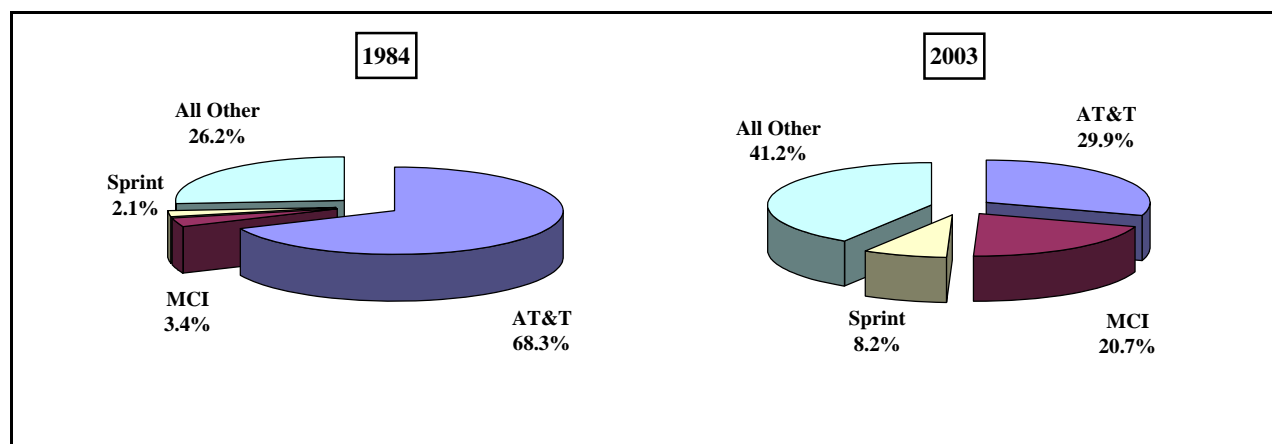
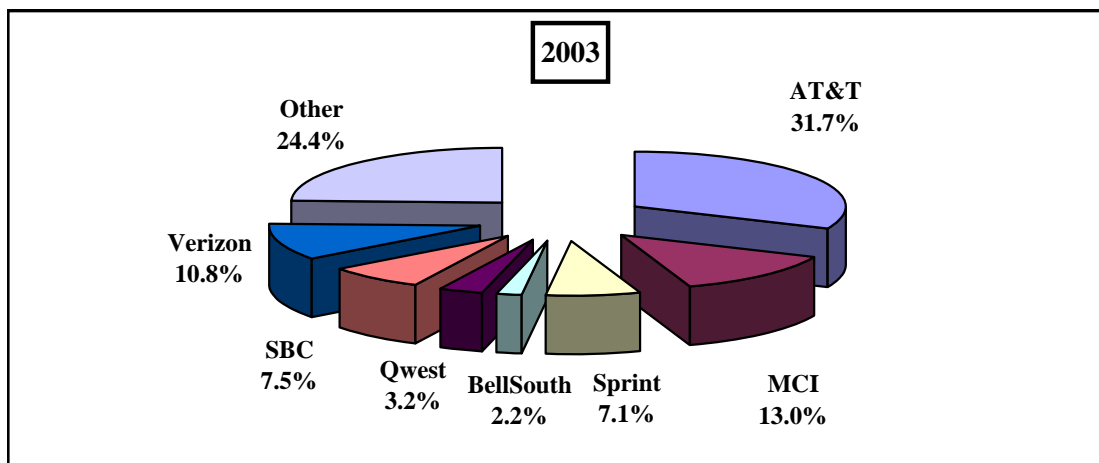


Table 9.7
Residential Household Market Shares
(1995 - 2003)

	AT&T ¹	MCI ²	Sprint	BellSouth ³	Qwest ⁴	SBC ⁵	Verizon ⁶	Other ⁷
Households ⁸								
1995	74.6 %	13.0 %	4.2 %	(7) %	(7) %	(7) %	(7) %	8.2 %
1996	69.9	14.1	5.0	(7)	(7)	(7)	(7)	11.0
1997	67.2	13.2	5.7	(7)	(7)	(7)	(7)	13.8
1998	62.6	15.1	5.7	(7)	(7)	(7)	(7)	16.6
1999	62.5	16.0	6.2	(7)	(7)	(7)	(7)	15.4
2000	51.1	18.0	6.6	0.1	1.6	1.0	4.6	17.0
2001	42.3	18.5	6.8	0.1	2.9	2.6	6.7	20.0
2002	36.7	15.8	7.6	0.2	2.5	3.8	9.3	24.1
2003	31.7	13.0	7.1	2.2	3.2	7.5	10.8	24.4
Direct Dial IntraLATA Minutes								
1995	8.9 %	2.4 %	4.6 %	(7) %	(7) %	(7) %	(7) %	84.1 %
1996	9.5	5.4	4.4	(7)	(7)	(7)	(7)	80.6
1997	13.9	6.7	3.7	(7)	(7)	(7)	(7)	75.7
1998	15.6	8.7	3.8	(7)	(7)	(7)	(7)	71.8
1999	16.9	12.0	3.6	(7)	(7)	(7)	(7)	67.5
2000	17.3	12.8	5.0	1.6	5.0	18.6	18.0	21.7
2001	15.4	13.2	4.8	1.4	4.3	17.9	17.6	25.3
2002	14.0	11.8	4.8	1.1	2.9	18.5	16.3	30.7
2003	10.7	11.4	8.1	0.9	2.7	17.7	13.2	35.4
Direct Dial InterLATA Minutes								
1995	69.5 %	16.1 %	5.8 %	(7) %	(7) %	(7) %	(7) %	8.6 %
1996	62.5	15.9	7.1	(7)	(7)	(7)	(7)	14.5
1997	62.4	14.9	6.5	(7)	(7)	(7)	(7)	16.2
1998	58.4	17.0	6.5	(7)	(7)	(7)	(7)	18.1
1999	53.2	20.9	6.6	(7)	(7)	(7)	(7)	19.3
2000	44.7	22.0	7.3	0.1	1.6	0.5	2.5	21.3
2001	36.3	20.5	7.6	0.1	1.9	1.8	3.6	28.1
2002	31.2	18.1	9.0	0.3	1.6	3.1	5.6	31.0
2003	26.0	16.6	7.9	1.4	1.8	6.6	6.6	32.9

Chart 9.3
Residential Household Market Shares



Notes for Table 9.7

Note: Market shares are estimates based on sample data. Shares for past years have been revised to take into account mergers and acquisitions and changes in methodology.

¹ AT&T Long Distance, Lucky Dog Phone Co. and ACC Long Distance

² MCI Long Distance, Telecom USA, Touch 1, TTI National, LDDS WorldCom and WorldCom Network Service

³ BellSouth Long Distance and BellSouth Public Communications

⁴ Qwest and U S WEST Long Distance

⁵ Ameritech Communications, Ameritech 800, Pacific Bell, Southwest Long Distance, SBC Long Distance and SNET All Distance

⁶ Bell Atlantic Long Distance, NYNEX/Bell Atlantic North, Verizon Select Services and GTE

⁷ Until 2000, the regional Bell operating companies are not broken out of the "Other" category.

⁸ Each household is assumed to have a single access line (less than 8% of households in the 2003 sample had more than one access line). These lines are allocated across carriers based on the household's primary long distance carrier which is imputed by the provider of the data, TNS Telecoms. In 1995, 1996 and 1999-2003, TNS defined the household's primary long distance carrier. In 1997, a household's primary long distance carrier was determined based on calls made through long distance carriers, and in 1998, a household's primary long distance carrier was determined based on interLATA calls.

Source: Calculated by Industry Analysis and Technology Division staff using survey data from TNS Telecoms *ReQuest Market Monitor*™, *Bill Harvesting*®.

EXHIBIT “FF”

Telecoms let NSA spy on calls; AT& T, MCI, Sprint cooperate with warrantless surveillance, execs say USA TODAY
February 6, 2006 Monday

gence director

Sources: Specter on NBC's Meet the Press; Hayden on ABC's This Week

LOAD-DATE: February 6, 2006

6 of 6 DOCUMENTS

Copyright 2006 Gannett Company, Inc.
All Rights Reserved
USA TODAY

February 6, 2006 Monday
FINAL EDITION

SECTION: NEWS; Pg. 1A

LENGTH: 667 words

HEADLINE: Telecoms let NSA spy on calls;
AT&T, MCI, Sprint cooperate with warrantless surveillance, execs say

BYLINE: Leslie Cauley and John Diamond

BODY:

The National Security Agency has secured the cooperation of large telecommunications companies, including AT&T, MCI and Sprint, in its efforts to eavesdrop without warrants on international calls by suspected terrorists, according to seven telecommunications executives.

The executives asked to remain anonymous because of the sensitivity of the program.

AT&T, MCI and Sprint had no official comment.

The Senate Judiciary Committee begins hearings today on the government's program of monitoring international calls and e-mails of a domestic target without first obtaining court orders.

At issue: whether the surveillance is legal, as President Bush insists, or an illegal intrusion into the lives of Americans, as lawsuits by civil libertarians contend. In domestic investigations, phone companies routinely require court orders before cooperating.

A majority of international calls are handled by long-distance carriers AT&T, MCI and Sprint. All of the carriers own "gateway" switches capable of routing calls to points around the globe.

AT&T was recently acquired by SBC Communications, which has since adopted the AT&T name as its corporate moniker. MCI, formerly known as WorldCom, was recently acquired by Verizon. Sprint recently merged with Nextel.

The New York Times, which disclosed the clandestine operation in December, previously reported that telecommunications companies have been cooperating with the government, but it did not name the companies involved.

Decisions about monitoring calls are made in four steps, according to two U.S. intelligence officials familiar with the program who insisted on anonymity because it remains classified:

*Information from U.S. or allied intelligence or law enforcement points to a terrorism-related target either based in the United States or communicating with someone in the United States.

Telecoms let NSA spy on calls; AT&T, MCI, Sprint cooperate with warrantless surveillance, execs say USA TODAY
February 6, 2006 Monday

*Using a 48-point checklist to identify possible links to al-Qaeda, one of three NSA officials authorized to approve a warrantless intercept decides whether the surveillance is justified. Gen. Michael Hayden, the nation's No. 2 intelligence officer, said the checklist focuses on ensuring that there is a "reasonable basis" for believing there is a terrorist link involved.

*Technicians work with phone company officials to intercept communications pegged to a particular person or phone number. Telecommunications executives say MCI, AT&T and Sprint grant the access to their systems without warrants or court orders. Instead, they are cooperating on the basis of oral requests from senior government officials.

*If the surveillance yields information about a terrorist plot, the NSA notifies the FBI or other appropriate agencies but does not always disclose the source of its information. Call-routing information provided by the phone companies can help intelligence officials

eavesdrop on a conversation. It also helps them physically locate the parties, which is important if cellphones are being used. If the U.S. end of a communication has nothing to do with terrorism, the identity of the party is suppressed and the content of the communication destroyed, Hayden has said.

The government has refused to publicly discuss the precise number of individuals targeted.

The Times and The Washington Post have said thousands have had communications intercepted.

The two intelligence officials said that number has been whittled down to about 600 people in the United States who have been targeted for repeated surveillance since the Sept. 11 attacks.
Surveillance hearings open today

When: 9:30 a.m. ET today; TV: C-SPAN

Where: Senate Judiciary Committee

Questioners:

10 Republicans and eight Democrats

Witness: Attorney General Alberto Gonzales

Issue: Are warrantless wiretaps legal in the fight against terrorism?

"It is in flat violation" of the law.

-- Arlen Specter,

R-Pa., Judiciary

Committee

chairman

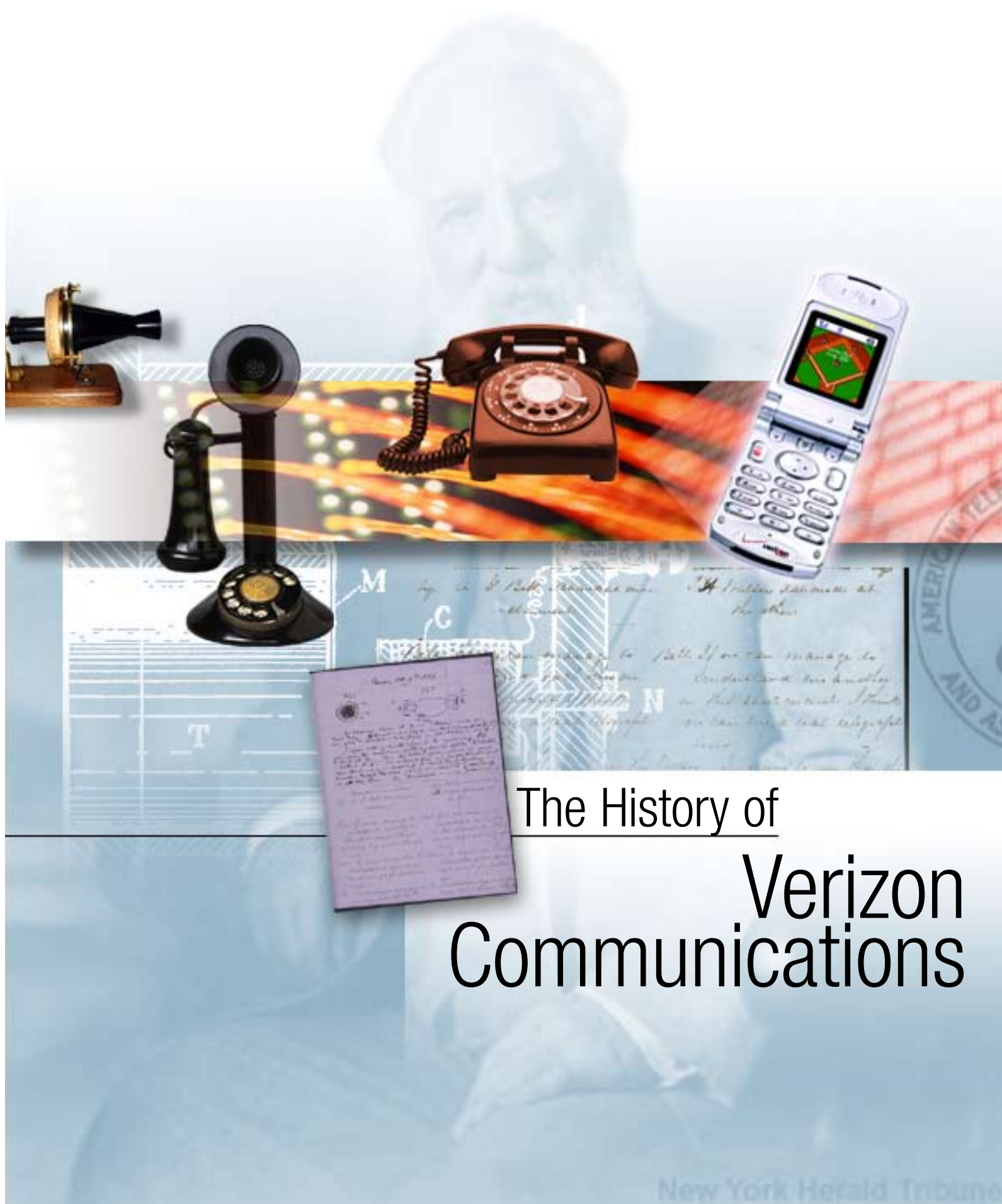
"It's about hot pursuit of al-Qaeda communications."

-- Gen. Michael

Hayden, deputy

national intelli-

EXHIBIT “GG”



The History of Verizon Communications



Verizon Communications Inc., based in New York and incorporated in Delaware, was formed on June 30, 2000, with the merger of Bell Atlantic Corporation and GTE Corporation. Verizon began trading on the New York Stock Exchange (NYSE) under its new "VZ" symbol on Monday, July 3, 2000.

The symbol was selected because it uses the two letters of the Verizon logo that graphically portray speed, while also echoing the genesis of the company name: veritas, the Latin word connoting certainty and reliability, and horizon, signifying forward-looking and visionary.

While Verizon is truly a 21st century company, the mergers that formed Verizon were several years in the making, involving companies with roots that can be traced to the beginnings of the telephone business in the late 19th century.

Government regulation largely shaped the evolution of the industry throughout most of the 20th century. Then, with the signing of the Telecommunications Act on Feb. 8, 1996, federal law directed a shift to more market-based policies. This promise of a new competitive marketplace was a driving force behind Verizon's formation.

The Bell Atlantic - GTE Merger

The mergers that formed Verizon were among the largest in U.S. business history, culminating in a definitive merger agreement, dated July 27, 1998, between Bell Atlantic, based in New York City, and GTE, which was in the process of moving its headquarters from Stamford, Conn., to Irving, Texas.

GTE and Bell Atlantic had each evolved and grown through years of mergers, acquisitions and divestitures. Each had proven track records in successfully integrating business operations.

Prior to the merger, GTE was one of the world's largest telecommunications companies, with 1999 revenues of more than \$25 billion. GTE's National and International Operations served approximately 35



million access lines through subsidiaries in the United States, Canada and the Dominican Republic, and through affiliates in Canada, Puerto Rico and Venezuela.



(Access lines are the individual connections from a customer's premises to the phone network.) GTE was a leading wireless operator in the United States, with more than 7.1 million wireless customers and the opportunity to serve 72.5 million potential wireless customers.

Outside the 50 states, GTE operated wireless networks serving approximately 6.7 million customers with 34.8 million potential wireless customers through subsidiaries in Argentina, Canada and the Dominican Republic, and affiliates in Canada, Puerto Rico, Venezuela and Taiwan. GTE provided internetworking services, ranging from dial-up Internet access for residential and small-business consumers to Web-based



1876

In Boston, Alexander Graham Bell transmits the first complete message - "Mr. Watson, come here, I want you!" - with the use of his invention, the telephone.

1885

American Telephone and Telegraph Co. is established

1910

The Interstate Commerce Commission (ICC) assumes jurisdiction over interstate telephone companies

HISTORY OF VERIZON COMMUNICATIONS INC.

applications for Fortune 500 companies. GTE was also a leader in directories and telecommunications-based information services and systems.

Bell Atlantic was even larger than GTE, with 1999 revenues of more than \$33 billion. Its Domestic Telecom unit served 43 million access lines, including 22 million households and more than 2 million business customers. Its Global Wireless unit managed one of the world's largest and most successful wireless companies, with 7.7 million Bell Atlantic Mobile customers in the United States, and international wireless investments in Latin America, Europe and the Pacific Rim.

Bell Atlantic's Directory Services was already the world's largest publisher of directory information, including operations in Europe. Bell Atlantic's International unit included a mix of mature and start-up wireline telecommunications investments in Europe and the Pacific Rim. In total, Bell Atlantic held assets of more than \$62 billion, and the company was investing to strengthen its core telecom and wireless businesses and to accelerate growth by extending its reach into data, e-commerce and new wireless markets.

The Bell Atlantic - GTE transaction — valued at more than \$52 billion at the time of the announcement — was designed to join Bell Atlantic's sophisticated network serving its densely-packed, data-intensive customer base in 13 states from Maine to the Virginias with GTE's national footprint, advanced data communications capabilities and long-distance expertise. The purpose was to create a combined company with the scale and scope to compete as one of the telecommunications industry's top-tier companies. This combined company would be able to provide long-distance and data services nationwide as part of a full package of other communications services (subject to regulatory restrictions).

The merger closed nearly two years later, following review and approvals by Bell Atlantic and GTE shareholders, 27 state regulatory commissions and the Federal Communications Commission (FCC), and clearance from the U.S. Department of Justice (DOJ) and various international agencies.

In the meantime, on Sept. 21, 1999, Bell Atlantic and London-based Vodafone AirTouch Plc (now Vodafone Group Plc) announced that they had agreed to create a new wireless business — with a national footprint, a single brand and a common digital technology — composed of Bell Atlantic's and Vodafone's U.S. wireless assets (Bell Atlantic Mobile, AirTouch Cellular, PrimeCo Personal Communications and AirTouch Paging).

This wireless joint venture received regulatory approval in six months. The new "Verizon" brand was launched on April 3, 2000, and the wireless joint venture began operations as Verizon Wireless on April 4, 2000. GTE's wireless operations became part of Verizon Wireless — creating the nation's largest wireless company — when the Bell Atlantic - GTE merger closed nearly three months later. Verizon then became the majority owner (55 percent) of Verizon Wireless.

When Verizon Communications began operations in mid-2000, the leaders of Bell Atlantic and GTE shared management responsibility for the company. Former GTE Chairman and CEO Charles R. "Chuck"

TELECOM TIMELINE



Lee became Verizon's founding Chairman of the Board and co-CEO, while former Bell Atlantic CEO Ivan Seidenberg became Verizon's founding President and co-CEO. In accordance with a leadership transition plan announced at the time of the merger, Lee retired from Verizon in 2002. Seidenberg is currently Chairman and CEO.

Recent Verizon History

A bellwether for the industry, Verizon Communications was added to the Dow Jones Industrial Average in 2004. Verizon continues to have a nationwide presence in wireline and wireless markets, with approximately more than 100 million Americans connecting to a Verizon network daily. With the addition of MCI, Inc., in 2006, Verizon is now also a leading provider of advanced communications and information technology solutions to large business and government customers worldwide.

As of year-end 2006, Verizon's wireline network included more than 45 million wireline access lines and 7 million broadband connections nationwide. Over 1.2 billion phone calls and trillions of bits of data were being carried over this nationwide network on an average business day, with a reliability factor of over 99.99 percent. Verizon's wireline network also included approximately 13 million miles of local, inter-city and long-distance fiber-optic systems -- more than enough to circle the Earth 520 times.

Meanwhile, Verizon Wireless owned and operated the nation's most reliable wireless network. By year-end 2006, Verizon Wireless served more than 59 million customers in 49 of the top 50 U.S. markets. Verizon's wireless network is 100 percent digital, with more than 170 switching facilities nationwide.

In 2005 and 2006, Verizon invested a total of more than \$32 billion to maintain, upgrade and expand its technology infrastructure. Verizon's strong cash flow from operating activities (\$23 billion in 2006) has enabled the company to maintain a healthy level of investment in growth areas -- particularly broadband and wireless -- even as the company has reduced total debt significantly through the decade. At the same time, Verizon has shed non-strategic assets and investments. For example, Verizon sold wireline access lines in Alabama, Missouri and Kentucky in 2002 and in Hawaii in 2005.

In 2006, Verizon spun off its U.S. print and Internet yellow pages directories company to Verizon shareholders. The spin-off resulted in a new public company called Idearc Inc. (pronounced EYE-dee-ark). Verizon shareholders received one share of Idearc common stock for every 20 shares of Verizon common stock, and Idearc began trading on the NYSE as a separate company on Nov. 20.

When Verizon Communications began operations in mid-2000, the leaders of Bell Atlantic and GTE shared management responsibility for the company. Former GTE Chairman and CEO Charles R. "Chuck" Lee became Verizon's founding Chairman of the Board and co-CEO, while former Bell Atlantic CEO Ivan Seidenberg became Verizon's founding President and co-CEO. In accordance with a leadership transition plan announced at the time of the merger, Lee retired from Verizon in 2002. Seidenberg is currently Chairman and CEO.



Also in 2006, Verizon reached definitive agreements to sell its interests in telecommunications providers in the Dominican Republic, Puerto Rico and Venezuela in three separate transactions to América Móvil, a wireless service provider throughout Latin America, and a company owned jointly by Teléfonos de México (Mexico's leading full-service telecommunications company) and América Móvil. The sale of Verizon Dominicana closed on Dec. 1, and the other transactions were still pending by year-end.

In 2004, Verizon began major initiatives, which continue today, to bring next-generation broadband services (wireless EV-DO and fiber-optic-based FiOS services) to wireless and wireline customers in the United States. By year-end 2006, Verizon's broadband wireless network was available to more than 200 million Americans, with EV-DO enhancements announced early in 2007. For wireline customers, Verizon is the only major U.S. telecommunications company building an advanced, all-digital fiber-optic network, on a mass scale, all the way to customers' homes. From 2004 through 2010, the company plans to invest \$22.9 billion -- or \$18 billion in addition to normal network investment costs -- to deploy Verizon's fiber network past approximately 18 million premises and attract up to 7 million FiOS Internet customers and up to 4 million FiOS TV customers.

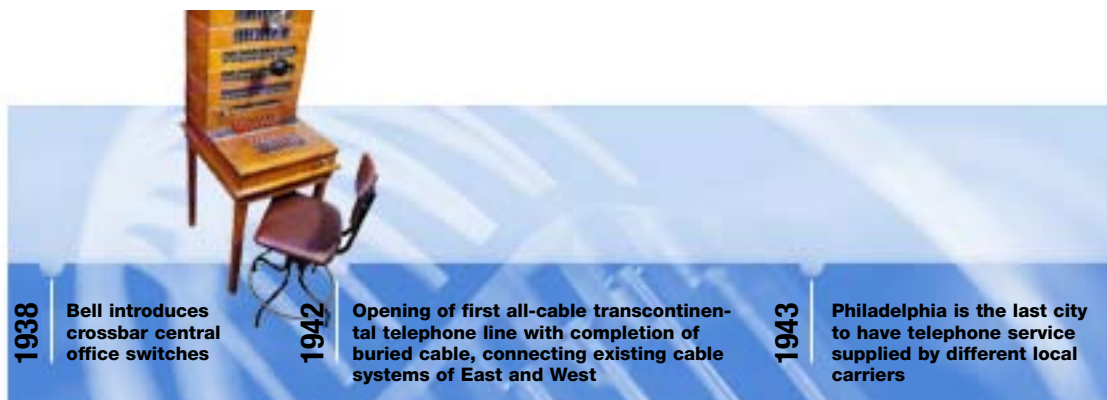
The MCI Merger

On Feb. 14, 2005, Verizon announced that it had agreed to acquire MCI, in a move to enhance Verizon's ability to deliver the benefits of converged communications, information and entertainment across the country and around the world.

Qwest Communications later announced a separate bid for MCI, but in May 2005 the MCI Board endorsed an amended bid by Verizon. MCI shareholders approved the merger with Verizon in October 2005, and state, federal and international regulatory approvals were obtained by year-end 2005. The merger closed on Jan. 6, 2006, in a transaction valued at approximately \$8.5 billion.

With this transaction, Verizon had \$88.1 billion in 2006 total consolidated operating revenues, and at year-end 2006 the company had approximately 242,000 employees, serving customers in more than 140 countries. Verizon currently operates two network-based business units: Verizon Wireless, operator of America's most reliable wireless network; and Wireline, including Verizon Telecom, which is deploying the most advanced wireline broadband and video network in America today, and Verizon Business, which includes many former MCI operations and serves medium and large businesses and government customers.

Current facts and figures about Verizon can be obtained at <http://newscenter.verizon.com/kit/vcorp/fact-sheet.shtml> and additional details about Verizon Wireless can be obtained at http://news.vzw.com/pdf/Verizon_Wireless_Press_Kit.pdf



The Diverse Legacies of Bell Atlantic and GTE

On the day Verizon Communications was incorporated, it included almost all operations of the former Bell Atlantic and the former GTE. The company was structured just as it is today, with four business segments: Domestic Telecom, Verizon Wireless, International and Information Services. Some overlapping wire- less properties were divested as one of the DOJ's conditions for merger approval. One FCC condition for merger approval — a spin-off of more than 90 percent of GTE's Internet infrastructure business — illus- trates an important difference between the legacies of Bell Atlantic and GTE: Bell Atlantic was a “Baby Bell,” while GTE was the largest “independent” telecommunications company.

Bell Atlantic: Former Baby Bell

The term “Baby Bell” — synonymous with RBOC, or Regional Bell Operating Company — indicates that Bell Atlantic was one of the companies tracing its heritage to the Bell System, which was a common name for the organizational structure of the American Telephone and Telegraph Co. (AT&T) prior to 1984.

Until then — as the result of a 1913 agreement known as the Kingsbury Commitment and reinforced by the Communications Act of 1934 (the act that created the FCC) — the Bell System functioned as a legally sanctioned, regulated monopoly. The purpose of this sanction was the goal of “Universal Service” which, according to the 1934 Act, was “to make available...for all the people of the United States a rapid, effi- cient nationwide...wire and radio communication service with adequate facilities at reasonable charge.”

On Jan. 1, 1984, 22 local telephone companies were split from parent company AT&T. At the time, it was the largest private business enterprise in the world, with more than 1 million U.S. employees; the com- pany was popularly referred to as “Ma Bell.”

A divestiture occurs when one or more companies are split from a parent corporation, often by govern- ment order. The divestiture of AT&T was so large and unprecedented that it became known as simply “Divestiture.” Events leading to Divestiture included the FCC's 1968 Carterfone decision, which allowed competition with the Bell System for telephone equipment, and a 1974 antitrust suit filed by the DOJ, charging that AT&T had unlawfully monopolized the telecommunications market. After years of preparation and several months of trials related to this antitrust suit, the government and AT&T resolved their differenc- es out of court, agreeing to a consent decree in January 1982. This is also sometimes called the Modified Final Judgment, or MFJ, since the settlement modified a 1956 consent decree also involving AT&T.

According to terms of Divestiture, the 22 operating Bell telephone companies were formed into seven regional holding companies of roughly equal size. Bell Atlantic was one of the original seven RBOCs, or Baby Bells, that began operations in 1984.



When it was formed, Bell Atlantic was based in Philadelphia and consisted of several telephone companies (Bell of Pennsylvania; C&P Telephone Companies of D.C., Maryland, Virginia and West Virginia; Diamond State Telephone, and New Jersey Bell) serving six states (Delaware, Maryland, New Jersey, Pennsylvania, Virginia and West Virginia) and the District of Columbia.

One key regulatory restriction imposed by Divestiture on all of the RBOCs was a prohibition against providing long-distance telephone services in their own jurisdictions. The MFJ had divided the United States into geographic areas within which an RBOC could offer telecommunications services. These areas are called Local Access and Transport Areas, or LATAs. Local telecommunications services are called intra-LATA, while long-distance services are called interLATA. (Area codes and LATAs do not necessarily share boundaries; New York state, for example, has eight LATAs and a dozen area codes. A similar and frequently-used industry abbreviation is NNX, which refers to the three digits that follow an area code in a 10-digit phone number.)

GTE: The Largest Independent

There were more than 1,400 local phone companies in 1984 that were never part of the Bell System. Many still exist today, primarily in rural areas. Typical independents are family-owned businesses or subscriber-owned cooperatives that serve one or more small communities.

The independent telephone industry originated in 1893, when Alexander Graham Bell's original patents expired. In the early years of this industry, customers of independent telephone companies could only call other customers served by the same company.

GTE, before its merger with Bell Atlantic, was the largest independent phone company in the United States, owning numerous independent local telephone properties in rural and urban areas from Hawaii and California to Virginia.

This distinction between "former Bell System" and "independent" meant that Bell Atlantic and GTE had historically been regulated very differently. For example, GTE was already providing long-distance (inter-LATA) services to customers at the time the merger with Bell Atlantic was announced. GTE had owned and operated the Sprint long-distance network during parts of the 1980s and 1990s. However, as a result of a consent decree entered into by GTE in connection with its acquisition of the Sprint network, GTE was required to keep its Sprint business separate from the business conducted by its telephone operating companies. GTE re-entered the long-distance business in conjunction with its local telephone operations shortly after the Telecommunications Act of 1996 eliminated these separation restrictions.

On the other hand, as a former Baby Bell, Bell Atlantic's entry into the long-distance business had been subject to greater restrictions. Under Section 271 of the Telecommunications Act, federal regulators must certify, with input from state regulators and the DOJ, that local telecommunications markets are fully open to competition before a former Baby Bell can be approved to offer long-distance service in a jurisdiction.



Bell Atlantic was the first of the former Baby Bells to file a Section 271 application that was approved by the FCC, and the company had entered the long-distance market in New York state in January 2000. However, at the time of the Bell Atlantic - GTE merger in June 2000, regulators did not want to allow Verizon to have operational control of GTE's Internet infrastructure business, which operated across LATA boundaries in all states, before Verizon had Section 271 approvals in almost all of the former Bell Atlantic states (which occurred in 2003). Therefore, one condition to the FCC's approval of the Bell Atlantic - GTE merger was the spin-off of this interLATA data business — an independent company called Genuity.

The History of Bell Atlantic

One of the most significant evolutionary steps for Bell Atlantic was a June 1994 agreement to form a wireless joint partnership with NYNEX, another of the original seven Baby Bells that began operations in 1984. The combined wireless businesses were to cover 55 million potential customers along the East Coast and in the Southwest. This combination began operations in July 1995 under the name Bell Atlantic NYNEX Mobile.

NYNEX (pronounced "NINE-x"), based in New York, was so named because it was composed of the New York and New England telephone companies that were formerly part of the Bell System ("NY" representing New York, "NE" representing New England, and "X" the undefined future). It operated in seven Northeastern states — Connecticut, Maine, Massachusetts, New Hampshire, New York, Rhode Island and Vermont. For a decade, New York Telephone and New England Telephone were branded independently, but under Ivan Seidenberg's direction, operations were internally "merged" under a single NYNEX brand on Jan. 1, 1994.

The Bell Atlantic - NYNEX wireless partnership marked the beginnings of the current-day Verizon Wireless.

This partnership also began a relationship between the two RBOCs that resulted in an announcement on April 22, 1996, that Bell Atlantic and NYNEX had agreed to merge their entire operations in a transaction then valued at \$23 billion. On April 1, 1996 — less than two months after the signing of the Telecommunications Act — two other Baby Bells (SBC Communications and Pacific Telesis) had also proposed a merger, and more than a year of regulatory review and approvals followed for each.

The Bell Atlantic - NYNEX merger united a natural market in the adjoining Northeast and Mid-Atlantic regions. The "new" Bell Atlantic opened for business on Aug. 15, 1997. As announced when the merger agreement was struck, the company retained the Bell Atlantic name and was headquartered in New York. Raymond W. Smith retained the title of Chairman and CEO of Bell Atlantic after the merger, and Seidenberg, who was formerly Chairman and CEO of NYNEX, became the Vice Chairman, President and Chief Operating Officer. Seidenberg was later named CEO, then Chairman upon Smith's retirement at the end of 1998.

Even before their merger, both Bell Atlantic and NYNEX had been making headlines since the 1984 Divestiture. Under Seidenberg, NYNEX was widely recognized as among the first of the Baby Bells to embrace the new



competitive era codified by the Telecommunications Act of 1996, and throughout the '90s Bell Atlantic's Smith articulated a vision for the Information Superhighway made possible by the fledgling Internet.

The companies produced a string of "firsts" in the post-Divestiture telecommunications industry. Bell Atlantic was the first in the nation to offer Caller ID service, which was introduced in New Jersey in 1988. In 1990, Delaware became the first state with border-to-border cellular service, which was provided by Bell Atlantic Mobile. In 1993, NYNEX introduced the technology of voice-activated dialing into the "public switched network," the predominantly landline network that is accessible to anyone using a telephone.

Also in 1993, Bell Atlantic proposed a merger with cable TV giant Tele-Communications Inc. — a high-profile deal later terminated by Bell Atlantic, but one that dramatically accelerated the pace of change in the industry, making it clear that convergence of digital technologies and industry consolidation were the way of the future.

Bell System History

Before 1984, as part of the Bell System, the histories of Bell Atlantic and NYNEX followed similar paths. They were, in fact, part of one management system, promulgated in 1908. Theodore N. Vail, the then-new president of AT&T, set forth a vision that would define the Bell System for many years to come — "One Policy, One System, Universal Service."

The Bell System has a long and storied history, dating back to the very invention of the telephone and the first patent filed by Bell, applied for on Feb. 14, 1876, and granted on March 7, 1876. Three days later, the inventor dropped a battery, spilling acid. He called out to his assistant, "Mr. Watson, come here!" and Watson heard Bell's words over the new device.

Many books and other educational resources are available that chronicle the history of the Bell System — from 1917 when exchange names ("Pennsylvania 6") were first added to four-digit phone numbers in New York (a practice that began to be phased out in 1960 with the introduction of "all number calling"), to the first public demonstration of the newly invented transistor by Bell Telephone Laboratories in 1948, to the introduction of Picturephone service coincident with the 1964 World's Fair.

An underlying theme of Bell System culture has been an attention to customer service — whether exhibited by a bedrock commitment to protect customer privacy or by the heroic efforts of phone company managers and technicians to restore essential services following disasters.

This service ethic is often depicted by a Bell System-commissioned painting, "The Spirit of Service," based on a photograph of New England Bell lineman Angus Macdonald in snowshoes, maintaining the only long-distance telephone lines between New York and Boston during the Great Blizzard of 1888. Bell



System communications lines had stayed open during the severe March storm that otherwise had paralyzed the Northeast.

Examples of the Spirit of Service abound throughout the history of the Bell Atlantic and NYNEX telephone companies. On Feb. 27, 1975, a fire of unknown origin swept through a New York Telephone central office in lower Manhattan, causing the worst service disaster ever suffered by a single Bell operating company. The company restored lines serving more than 170,000 phones within 22 days — a technological feat that, at the time, would normally have taken a year or more. The restoration effort was dubbed “The Miracle of Second Avenue.”

More recently, this spirit was exemplified by Verizon’s restoration efforts following the terrorist attacks on Sept. 11, 2001.

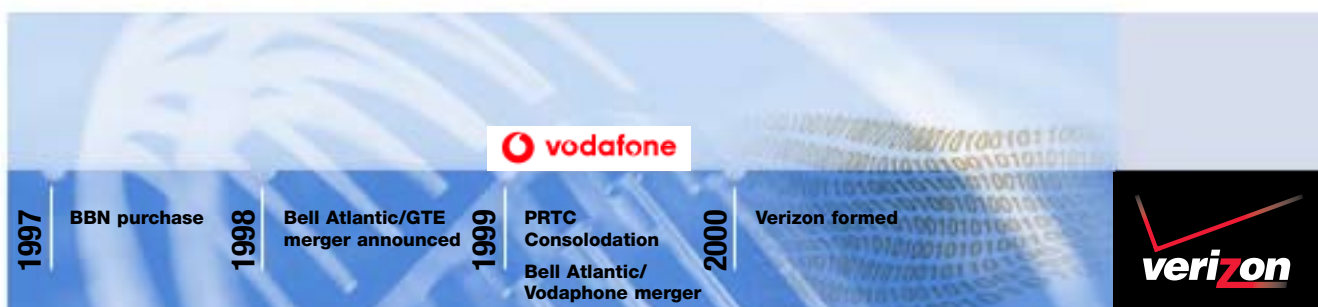
These restoration efforts were enhanced by the scale and scope Verizon had obtained through the merger of Bell Atlantic and GTE, together with the cooperation of other companies in a now fully competitive industry. In New York, Verizon employees responded to the emergency by helping the NYSE resume trading and handle record volumes less than a week after the attacks on the World Trade Center. At crash sites in Pennsylvania and at the Pentagon, employees provided emergency services and rebuilt systems. In less than 90 days, Verizon had restored a phone and data network at Ground Zero of roughly the size and complexity of one serving a city the size of Cincinnati. [More information about this effort can be found at <http://newscenter.verizon.com/wtc2/>]

The History of GTE

The early GTE structure was forged primarily through an aggressive history of acquisitions and mergers — beginning with the acquisition of hundreds of small telephone companies independent of the Bell System. These companies had been formed following the 1894 expiration of the last of the telephone patents granted to Bell. This expansion movement reached its zenith in the late 1950s with the combination of three large corporations that formed the nucleus of the GTE as it was structured in 1990: General Telephone, Theodore Gary and Co., and Sylvania Electric Products Inc.

GTE was conceived as a corporate entity in 1918 when John F. O’Connell, Sigurd L. Odegard and John A. Pratt purchased the small Richland Telephone Co. in Wisconsin. The partnership became a corporation two years later, with the acquisition of other Wisconsin telephone properties. Later, the corporation purchased a Long Beach, Calif., telephone company, and a holding company called Associated Telephone Utilities Co. was organized in 1926 to serve as an umbrella for the Wisconsin and California properties.

Associated Telephone Utilities served 500,000 telephones before the stock market crash of 1929 and the Great Depression that followed. Depleted financial resources forced the corporation into receivership in 1933, but it emerged two years later, reorganized as General Telephone Corp.



HISTORY OF VERIZON COMMUNICATIONS INC.

The Missouri roots of Theodore Gary and Co. stretched back even further than those of Associated Telephone Utilities. Gary purchased the Macon, Mo., telephone exchange in 1897. Bitter competition developed when American Bell Telephone Co., AT&T's predecessor, tried to wipe out the independent telephone companies, sometimes leading to physical violence. The resolution of this conflict was the previously mentioned 1913 Kingsbury Commitment.

In the meantime, Gary was acquiring domestic and international telephone companies at a rapid rate. Theodore Gary and Co. and General Telephone were the two largest independent telephone companies in the United States when they merged in 1955.

Sylvania Electric Products began modestly in the 1910s in Massachusetts and Pennsylvania as a renewer of burnt-out light bulbs. Operations in both states moved on to production of new lamps and then to vacuum tubes in the 1920s, when radio broadcasting became increasingly popular. In 1931, the Massachusetts and Pennsylvania companies merged to become Hygrade Sylvania Corp., later Sylvania Electric Products. By the time it merged with General Telephone in 1959, Sylvania had become a leader in electronics, lighting, television and radio, and chemistry and metallurgy.

After this 1959 merger, the company became known as General Telephone & Electronics Corp. Donald C. Power, the first major architect of what was to become GTE, engineered General Telephone's mergers with Theodore Gary and Co. and Sylvania. As head of General Telephone, Power advocated a decentralized management, and operations of the three companies were not integrated. In addition to telephone company operations, the conglomerate-styled business participated in a diverse range of enterprises, producing a remarkable range of products over the following decades, including halogen automobile headlights, cutting tools, telecommunications equipment, cameras, television sets, atomic-reactor fuel elements, anti-missile defense systems, and space frame systems for buildings.

During this time, the holding company, based in New York, became known as GT&E Corp. In March 1970, blasts ripped through the headquarters buildings of GT&E and two other companies in New York; the terrorist group responsible was protesting the companies' participation in defense work at the height of the Vietnam War. In December 1970, GT&E announced that the company would move its world headquarters to Stamford, Conn. In 1971, the company adopted a new corporate symbol that became a widely recognized logo in the years to come, featuring the initials GTE placed inside a blue, rounded rectangle, and the company formally changed its name to GTE Corporation in 1982.

In 1981, the company sold its electronics holdings to North American Philips, a subsidiary of N.V. Philips, Europe's largest electronics company. Meanwhile, in moves in the telecommunications businesses, GTE Mobilnet was formed to construct and operate cellular systems in 1981 (the first customers were served in 1984 in the Indianapolis area, and in 1989 GTE was the first cellular provider to offer service nationwide). In 1983, the company bought infant long-distance carrier U.S. Sprint from Southern Pacific Co. Five years later, GTE sold its controlling interest in what was then called GTE Sprint to United Telecommunications Inc.; the remainder was sold in 1992.

11

TELECOM TIMELINE



By the end of the '80s, GTE was a corporation with annual revenues exceeding \$17 billion, employing more than 159,000 people in various telephone and manufacturing operations throughout the United States and some 40 other countries. GTE and its business operations had spanned the turbulent years from the industrial revolution to the beginnings of the information revolution.

GTE in the '90s

Under the leadership of James L. "Rocky" Johnson, who became GTE's Chairman and CEO in 1987, and Chuck Lee, who became Chairman and CEO-elect in late 1991, GTE focused its operations on local telecommunications and on the burgeoning market for data services. GTE anticipated the growing importance of telecommunications technology and the technological shift from analog to digital. By mid-decade, as data traffic was becoming more common than voice traffic on telephone networks, GTE was well positioned in key growth markets.

As early as 1990 in Cerritos, Calif., GTE began market testing of how to provide voice, data and video services over a range of transmission networks, including fiber optics, coaxial cable and the copper wiring traditionally used in the phone industry.

In March 1991, GTE acquired Contel Corp., which was the 10th largest telephone company in the United States and the 6th largest cellular provider. At the time, it was the largest merger in the history of the telecommunications industry. The transaction was valued at \$6.6 billion, and in its new form GTE became the largest U.S.-based local telephone company and the country's second largest mobile cellular company. (McCaw Cellular, which was subsequently purchased by AT&T, was the largest cellular company at the time.)

In January 1993, GTE sold its Sylvania lighting and related precision materials operations to OSRAM GmbH.

Later in 1993, GTE began offering Internet access services for residential and business customers. In 1997, GTE secured its position as a major provider of Internet services with the purchase of Internet pioneer BBN Corp.

In October 1997, GTE made headlines worldwide with a cash offer to acquire MCI Communications Corp., a long-distance company that had already been targeted for acquisition by British Telecommunications PLC and WorldCom Inc. In November, MCI accepted WorldCom's counter-offer.

In 1999, a GTE-led consortium completed the purchase of a controlling stake in the Puerto Rico Telephone Co. — the culmination of a series of complementary wireline and wireless acquisitions, partnerships and investments that Bell Atlantic and GTE had engaged in internationally, particularly in the Americas, prior to the close of the merger that formed Verizon.

Sources:

Verizon Media Relations, archived press releases.

The History of GTE: The Evolution of One of America's Great Corporations, by Thomas E. McCarthy, published by GTE Corporation, Stamford, CT, 1990.

Telephone: The First Hundred Years, by John Brooks, published by Harper & Row, New York, NY, 1976.

Events in Telecommunications History, published by AT&T, New York, NY, 1979 edition.

For further information, contact: robert.a.varettoni@verizon.com.

Updated February 2007

EXHIBIT “HH”

4 of 5 DOCUMENTS

Copyright 2007 Congressional Quarterly, Inc. All Rights Reserved. CQ Transcriptions

"All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published or broadcast without the prior written permission of CQ Transcriptions. You may not alter or remove any trademark, copyright or other notice from copies of the content."

March 20, 2007 Tuesday

TYPE: COMMITTEE HEARING

LENGTH: 29751 words

COMMITTEE: HOUSE JUDICIARY COMMITTEE

HEADLINE: REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE

SPEAKER:

REP. JOHN CONYERS JR., CHAIRMAN

LOCATION: WASHINGTON, D.C.

WITNESSES:

GLENN A. FINE, INSPECTOR GENERAL, DEPARTMENT OF JUSTICE
VALERIE CAPRONI, GENERAL COUNSEL, FBI

BODY:

HOUSE JUDICIARY COMMITTEE HOLDS A HEARING ON FBI PATRIOT
ACT MISUSE

MARCH 20, 2007

SPEAKERS:

REP. JOHN CONYERS JR., D-MICH.
CHAIRMAN

REP. HOWARD L. BERMAN, D-CALIF.

REP. RICK BOUCHER, D-VA.

REP. JERROLD NADLER, D-N.Y.

REP. ROBERT C. SCOTT, D-VA.

REP. MELVIN WATT, D-N.C.

REP. ZOE LOFGREN, D-CALIF.

REP. SHEILA JACKSON-LEE, D-TEXAS

REP. MAXINE WATERS, D-CALIF.

REP. MARTIN T. MEEHAN, D-MASS.

REP. BILL DELAHUNT, D-MASS.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

REP. ROBERT WEXLER, D-FLA.
 REP. LINDA T. SANCHEZ, D-CALIF.
 REP. STEPHEN I. COHEN, D-TENN.
 REP. HANK JOHNSON, D-GA.
 REP. LUIS V. GUTIERREZ, D-ILL.
 REP. BRAD SHERMAN, D-CALIF.
 REP. ANTHONY WEINER, D-N.Y.
 REP. ADAM B. SCHIFF, D-CALIF.
 REP. ARTUR DAVIS, D-ALA.
 REP. DEBBIE WASSERMAN-SCHULTZ, D-FLA.
 REP. KEITH ELLISON, D-MINN.

REP. LAMAR SMITH, R-TEXAS
 RANKING MEMBER
 REP. F. JAMES SENSENBRENNER JR., R-WIS.
 REP. HOWARD COBLE, R-N.C.
 REP. ELTON GALLEGLY, R-CALIF.
 REP. ROBERT W. GOODLATTE, R-VA.
 REP. STEVE CHABOT, R-OHIO
 REP. DAN LUNGREN, R-CALIF.
 REP. CHRIS CANNON, R-UTAH
 REP. RIC KELLER, R-FLA.
 REP. DARRELL ISSA, R-CALIF.
 REP. MIKE PENCE, R-IND.
 REP. J. RANDY FORBES, R-VA.
 REP. STEVE KING, R-IOWA
 REP. TOM FEENEY, R-FLA.
 REP. TRENT FRANKS, R-ARIZ.
 REP. LOUIE GOHMERT, R-TEXAS
 REP. JIM JORDAN, R-OHIO

*

CONYERS: Good morning. Committee will come to order.

We're here for a hearing on the inspector general's independent report on the FBI's use of national security letters.

Nearly six years ago, in the immediate aftermath of September 11th, the Department of Justice told us that they needed significantly enhanced authority, while promising the members of this committee in no uncertain terms that these new tools would be carefully and appropriately used.

Two years ago, when the Patriot Act was reauthorized, they promised us there was not a single instance in which the law had been abused.

Now, to underscore the importance of the reasons that we're holding this hearing, many of us remember the times in the past when the power of our government has been abused: in one war, led to the suspension of habeas corpus; another war, the notorious Palmer raids; in World War II, the internment of Japanese Americans; in the Vietnam War, the secret spying and enemy list.

In my view, we are now in a period where we risk a continuation of these deplorable acts and effect genuine harm

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

to the Constitution and the rule of law.

One week ago, the inspector general told us that the exact opposite was true of the promise that had been made that there was not a single instance when the Patriot Act was being reauthorized that the law had been abused.

One tool in particular, the national security letters -- essentially, secret subpoenas issued without any court review -- was used repeatedly to invade the privacy of law-abiding Americans outside the law and proper legal process.

This was a serious breach of trust. The department had converted this tool into a handy shortcut to illegally gather vast amounts of private information while at the same time significantly underreporting its activities to Congress.

CONYERS: We learned that the number of national security letter requests had increased from 8,500 in the year 2000 to in excess of 143,000 from the three-year period between 2003 and 2005.

The Department of Justice consistently provided inaccurate information to Congress concerning the national security letters, failing to identify at least 4,600 security letter requests to us.

The security letters were routinely issued without proper authorization, and outside statutory and regulatory requirements.

The inspector general found that more than 60 percent of the investigatory files they looked at included one or more violations of FBI policy.

But worse, the inspector general found even more widespread abuses concerning the so-called exigent letters, that is emergency requests for telephone and other data. An exigent letter, as opposed to a national security letter, is meant to obtain information in an extreme emergency, like a kidnapping when the bureau has already sought subpoenas for the requested information. But the FBI issued these letters in nonemergencies as a means to bypass the requirements of the national security letter procedure.

And so, as if it wasn't troubling enough, in many instances the bureau attempted to issue after-the-fact national security letters to cover their tracks on their use of exigent letters.

The inspector general specifically found that the exigent letters were ordinarily issued when there was no emergency present, and very often when there was not even a pending investigation.

More often than not, the letters were issued based on promises that subpoenas were in the process of being issued when that was not the case, and even though some subpoenas were never issued at all.

CONYERS: The Federal Bureau of Investigation made numerous factual misstatements in the letters, which were frequently issued in violation of the statute as well as the attorney general and FBI guidelines.

The recordkeeping was so poor that it was impossible for the I.G. to document how and why all these problems occurred.

And what disturbs me most is that the abuse and misuse of these security letters is not an isolated instance. It appears to be apparent of a pattern which the Department of Justice has violated not only our trust, but the very laws which they are charged with enforcing.

And so I hope -- from the approval of the notorious torture memos to warrantless and illegal surveillance to wrongful smearing of able U.S. attorneys, this Department of Justice has squandered its reputation for independence and integrity.

The attorney general needs to understand that with power comes responsibility and with authority must come

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

accountability.

I would like now to turn to the distinguished gentleman from Texas, the ranking member of this committee, Mr. Lamar Smith.

SMITH: Thank you, Mr. Chairman.

Mr. Chairman, I appreciate your holding this hearing on the inspector general's report on the FBI's use of national security letters. The inspector general should be commended for conducting a thorough audit as directed by Congress in the Patriot Act reauthorization.

The report raises concerns as to the FBI's internal recordkeeping and guidelines for the use of NSLs in terrorism and espionage investigations.

It is clear from the report that these deficiencies are the result of the poor implementation and administration of national security letter authority. In other words, the problem is enforcement of the law, not the law itself. Timely corrective measures by the FBI and effective oversight by the Justice Department and Congress will ensure proper use of this important law.

The inspector general's report found that the FBI's database for tracking NSLs significantly underestimated the number of NSL requests, resulting in inaccurate reports to Congress on the FBI's use of NSLs.

From 2003 to 2005, the FBI issued a total of 143,074 NSLs. This compares to 739 exigent letters to three telephone companies issued contrary to national security investigation guidelines. The exigent letters represent 1/200th of the national security letters issued.

Although the use of these unauthorized letters is disconcerting, the FBI discontinued this practice last year.

The inspector general makes two other very important findings.

First, there is no evidence that anyone at the FBI intended to violate the law or internal policy. This is a significant finding because it confirms that FBI agents acted in good faith and sought to comply with the law, even as they worked under severe time constraints and with an urgent desire to thwart terrorist activities.

Second, as detailed by the inspector general, NSLs are a critical tool in fighting terrorism and keeping our country safe. The information acquired through NSLs is valuable to international terrorism and espionage investigations and has allowed the FBI and intelligence agencies to identify terrorists and spies, the sources of their financing, and their plans to attack or harm our national security.

SMITH: In addition, the FBI shares important information gathered through NSLs with other intelligence agencies, joint terrorism task forces, and state and local law enforcement agencies.

To do their job, the FBI must be able to collect important information about suspected terrorists and spies while complying with the law and freely share such information with key partners.

In response to extensive oversight efforts conducted last Congress, the Patriot Reauthorization Act added critical new safeguards. For instance, an NSL recipient can challenge the request in court, nondisclosure orders require supervisory approval, and the recipient may disclose the NSL to an attorney.

I applaud the administration's response to the inspector general's report and expect the administration to follow through on its promise to act quickly to remedy the deficiencies identified by the inspector general.

Mr. Chairman, on September 11th, 2001, the United States was attacked. More than 3,000 people lost their lives.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

Members of Congress overwhelmingly approved important new counterterrorism tools for our nation's law enforcement personnel and updated existing authorities to meet the terrorist threat.

We must continue to demonstrate responsible leadership on the NSLs and other important national security issues.

Of course, we need to be vigilant to make sure these problems are fixed, that the inspector general's recommendations are implemented, and that our civil liberties and privacy are protected.

Mr. Chairman, I'll yield back the balance of my time.

CONYERS: And I thank the gentleman for his statement.

I'd like now to recognize the chairman of the Constitution Subcommittee, Jerry Nadler, for two and one-half minutes.

NADLER: Thank the chairman.

I'd like to thank Chairman Conyers for holding this important hearing on the FBI abuses of national security letters. We are here today in response to the Department of Justice inspector general report that found widespread abuses of the FBI's authority to issue national security letters.

And NSL can be issued to third party, such as a health insurance company or an Internet service provider, ordering them to reveal all their information about you and your transactions, and the third party is prohibited from telling you or anyone else about the order. That's the so-called gag order provision.

So you cannot object to an NSL directed at your information in court, as you could to a subpoena, because you don't know about it. And the third party may have no interest in going to court to protect your rights or your privacy.

While last year's reauthorization of the Patriot Act did make some changes to the NSL provisions, these changes were essentially meaningless. For example, the court is now authorized to modify or set aside the gag order only if it finds there is no reason to believe that disclosure would endanger national security, diplomatic relations, or anyone's life or safety. But the court must accept the government's assertion of harm as conclusive, so this protection is meaningless.

Some of us had predicted that the unrestricted authority of the FBI to issue NSLs would be abused. And unfortunately our worst fears have now been realized.

The I.G.'s audit found the NSLs have been used by the FBI to collect and retain private information about American citizens who are not reasonably suspected of being involved in terrorism.

During the last Congress, we predicted that unchecked power would lead to rampant abuse. That's why I proposed the Stop Self-Authorized Secret Searches Act two years ago. This bill would have restored some pre-Patriot Act provisions: that an NSL could not be issued unless the FBI made a factual, individualized showing that the records sought pertain to a suspected terrorist or spy. It would have given the recipient of a national security letter an opportunity to obtain legal counsel, the right to challenge the letter, and a nondisclosure requirement -- a real right to challenge it.

NADLER: It would have given notice to the target of the NSL if the government later seeks to use the records obtained from the NSL against him or her in a subsequent proceeding. And it would have given the target an opportunity to receive legal counsel and challenge the use of those records.

The bill would also have authorized the FBI to obtain documents that it legitimately needs while protecting the privacy of law-abiding American citizens.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

The abuses by the DOJ and the FBI are proving that these legislative fixes are a necessary check on the investigatory power. We do not trust government always to be run by angels, especially not this administration.

It is not enough to mandate that the FBI fix internal management problems and recordkeeping, because the statute itself authorizes the unchecked collection of information on innocent Americans. Congress must act now to fix the statute authorizing the abuses revealed in the I.G. report and to hold those responsible for these abuses and violations accountable.

Thank you. I yield back.

CONYERS: Thank you.

The chair recognizes the distinguished gentleman from Arizona, the ranking minority member of the Constitution Subcommittee, Trent Franks, for two and one-half minutes.

FRANKS: Well, thank you, Mr. Chairman.

Mr. Chairman, today our task is a vital one: to check and balance our sister branch of government through oversight and to ensure citizens' rights are being properly safeguarded.

Today's subject is somewhat delicate because we must all walk a fine line. In our grave and critical responsibility to prevent jihadist attacks upon American citizens, we must also be careful to strike the proper balance between vigilance and fighting the enemy on the one side of the scales and the preservation of citizens' rights on the other.

The report of the inspector general that we review today is hopeful. We see that while there are human imperfections in the FBI's operation, there was an overall finding that the FBI is indeed carrying out its duties responsibly, there being no evidence of any intentional or deliberate act to violate the law; and that NSLs are performing their vital function as a valuable tool in national security investigations.

FRANKS: To put today's hearing in perspective, we should keep in mind that the issuance of NSLs under the Patriot Act is a relatively new process, given that the Patriot Act is only a few years old and that this new use of NSLs will necessarily require a careful examination of their best and most appropriate use in this early period.

Certainly, we will have to work out the kinks, given that we are most likely in the business of fighting terror for a long time to come.

While the FBI's practices have had their shortcomings, it appears that these are problems that can be easily resolved. And this is good news. Many of the issues that we must review today are administrative in nature and, to some extent, unavoidable.

Government is a human institution, and it is therefore, by definition, imperfect. Those of us who have run corporations know that a perfect audit is a very rare occurrence, particularly on the first go-around.

Most business do internal audits -- perhaps many, many internal audits -- to discover where human judgment has fallen short and where to improve before being audited by an outside source.

This is an arduous but necessary task, and one that I hope we do well here today, and prospectively.

The FBI has vowed that it will make all the adjustments that Mr. Gonzales and Ms. Caproni have recommended. We look forward to the realization of this goal.

And with that, I thank the witnesses for joining us today, and we look forward to hearing your testimony.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

And thank you, Mr. Chairman.

CONYERS: Thank you.

The chair recognizes the distinguished gentleman from Virginia, Bobby Scott, chairman of the Crime Subcommittee, for two and a half minutes.

SCOTT: Thank you, Mr. Chairman.

Mr. Chairman, we all believe that it's important to be aggressive in fighting terrorism, and also aggressive in maintaining privacy and freedoms. And I don't believe we should operate on the premise that we always give up freedom in order to obtain security.

SCOTT: But for us to provide appropriate oversight, we have to have accurate information. Unfortunately, there are indications that we have received clearly inaccurate reports after the significant use of secret, invasive processes that do not appear to be necessary to advance terrorism-related investigations.

Whether it's a secret NSA wiretapping in violation of the FISA law or inappropriate use of the national security letters, we are discovering that what is actually occurring is quite different from what we were being told. And we cannot evaluate the ongoing need for NSA (sic) letters without accurate information.

There's also a clear indication of intentional misuse of the word "exigent" letters to telephone companies as emergency information when, in fact, no emergency existed. Somebody obviously knew this was a problem. There were, in fact, reports to Congress and oversight boards. And we need to find out who these people are.

With these disturbing indications, Mr. Chairman, I hope the testimony of the witnesses today will reveal who is responsible for these abuses and who should be held accountable for false reports to the Congress.

Thank you, Mr. Chairman. I yield back.

CONYERS: Thank you so much.

Another Virginian, the ranking minority member of the Crime Subcommittee, Mr. Randy Forbes?

FORBES: Mr. Chairman, I'd like to thank you and the ranking member, Congressman Smith, for holding this important hearing today and also for our witnesses for being here.

You know, the subject matter of this hearing makes for great theater, but when the show is over, we have the task of finding the facts and making sure the proper balance is struck and implemented to protect our citizens.

That we will do. And hopefully we will do it without the negativism and the emotionalism that seems so prevailing in public policy today. Pounding our fists makes great sound bites, but it does not stop terrorists or protect the privacy rights of our citizens.

It's clear that national security letters are important tools in international terrorism and espionage investigations conducted by the FBI. The inspector general's report, which details the audit of 77 case files in four field offices, shows a disturbing pattern: In 60 percent of those cases, the FBI's files were found to be in violation of the FBI's internal control policies for issuing national security letters.

FORBES: While the audit conducted concluded that there was no evidence of any intentional or deliberate act to violate the law, it's also clear that changes need to be made to the FBI's procedures so that they reflect the scope and intent of the law rather than the evolution of general practice.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

I look forward to hearing from the FBI about what procedures were in place during the time of the inspector general's audit; and how, given the inadequacies identified by the inspector general, the FBI plans to correct this.

Mr. Chairman, I yield back the balance of my time.

CONYERS: Thank you.

All other opening statements will be included in the record.

Mr. Glenn A. Fine, inspector general at the Department of Justice, a post held since he was confirmed by the Senate on December 15th, 2000. Mr. Fine's worked for the department's Office of Inspector General in a variety of capacities since January 1995. He's had several years in private practice, and also served as an assistant United States attorney in Washington, D.C.

We're also privileged to have with us the general counsel of the Federal Bureau of Investigation, Ms. Valerie Caproni, a position she's held since August 2003.

Prior to that, Ms. Caproni served as an assistant United States attorney in the Eastern District of New York, as a supervisor at the Securities and Exchange Commission, and also worked in private practice.

All your statements will be made a part of the record in their entirety. And we will have a five-minute time for each of you.

CONYERS: And we ask Inspector General Glenn A. Fine to begin our testimony.

Welcome to the committee.

FINE: Mr. Chairman, Congressman Smith and members of the Committee on the Judiciary, thank you for inviting me to testify about two reports issued by the Department of Justice Office of the Inspector General, regarding the FBI's use of national security letters and its use of Section 215 orders to obtain business records.

The Patriot Reauthorization Act required DOIG to examine the FBI's use of these authorities. And on March 9th, we issued reports detailing our findings.

Today I will summarize the key findings from our reviews, focusing my comments on the national security letter report.

Under five statutory provisions, the FBI can use national security letters -- NSLs -- to obtain, without review by a court, records such as customer information from telephone companies, Internet service providers, financial institutions and consumer credit companies.

Although most of the statutory provisions regarding NSLs existed prior to the enactment of the Patriot Act, the act significantly broadened the FBI's authority to use NSLs in two primary ways.

First, it eliminated the requirement that the information sought must pertain to a foreign power or an agent of a foreign power, and substituted the standard that the information requested must be relevant to or sought for an investigation to protect against terrorism or espionage.

Second, the Patriot Act significantly expanded approval authority for NSLs beyond a limited number of FBI headquarters officials to the heads of all FBI field officers.

Our review examined the FBI's use of NSLs from 2003 through 2005. The OIG will conduct another review, examining the FBI's use of NSLs in 2006, which we are required to issue by the end of this year.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

In sum, our review found widespread and serious misuse of the FBI's national security letter authorities.

In many instances, the FBI's misuse violated NSL statutes, attorney general guidelines, or the FBI's own internal policies.

FINE: We also found that the FBI did not provide adequate guidance, adequate controls or adequate training on the use of these sensitive authorities.

Before describing the main findings of our report, however, I believe it is important to provide context for these findings.

First, we recognize the significant challenges the FBI was facing during the period covered by our review. After the September 11th terrorist attacks, the FBI implemented major organizational changes while responding to continuing terrorist threats and conducting many counterterrorism investigations both internationally and domestically.

Second, it is also important to recognize that in most, but not all of the cases we examined, the FBI was seeking information it could have obtained properly through national security letters if it had followed applicable statutes, guidelines and internal policies.

Third, we did not find that the FBI employees sought to intentionally misuse NSLs or sought information that they knew they were not entitled to obtain. Instead, we believe the misuses and the problems we found generally were the product of mistakes, carelessness, confusion, sloppiness lack of training, lack of adequate guidance and lack of adequate oversight.

I do not believe that any of my observations, however, excuses the FBI's misuse of national security letters.

When the Patriot Act enabled the FBI to obtain sensitive information through NSLs on a much larger scale, the FBI should have established sufficient controls and oversight to ensure the proper use of those authorities. The FBI did not do so.

The FBI's failures, in my view, were serious and unacceptable.

I would now like to highlight our review's main findings.

Our review found that after enactment of the Patriot Act, the FBI's use of national security letters increased dramatically.

In 2000, the last full year prior to passage of the Patriot Act, the FBI issued approximately 8,500 NSL requests. After the Patriot Act, the number of NSL requests increased to approximately 39,000 in 2003, approximately 56,000 in 2004, and approximately 47,000 in 2005.

In total, during the three-year period, the FBI issued more than 143,000 NSL requests.

FINE: However, we believe that these numbers, which are based on information from the FBI's database, significantly understate the total number of NSL requests.

During our file reviews in four FBI field offices, we found additional NSL requests in the files than were contained in the FBI database. In addition, many NSL requests were not included in the department's reports to Congress.

Our review also attempted to assess the effectiveness of national security letters. NSLs have various uses, including to develop links between subjects of FBI investigations and other individuals and to provide leads and evidence to allow FBI agents to initiate or close investigations.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

Many FBI headquarters and field personnel from agents in the field to senior officials told the OIG that NSLs are indispensable investigative tools in counterterrorism and counterintelligence investigations, and they provided us with examples and evidence of the importance to these investigations.

The OIG review also examined whether there were any improper or illegal uses of NSL authorities. From 2003 through 2005, the FBI identified 26 possible intelligence violations involving its use of NSLs.

We visited four FBI field offices and reviewed a sample of 77 investigative case files and 293 NSLs. We found 22 possible violations that had not been identified or reported by the FBI.

We have no reason to believe that the number of violations we identified in the field offices was skewed or disproportionate to the number of violations in other files. This suggests that the large number of NSL-related violations throughout the FBI have not been identified or reported by FBI personnel.

In one of the most troubling findings, we determined that the FBI improperly obtained telephone toll billing records and subscriber information from three telephone companies pursuant to over 700 so-called exigent letters. These letters generally were signed by personnel in the Communications Analysis Unit, the CAU, a unit of the Counterterrorism Division in FBI headquarters.

The exigent letters were based on a form letter used by the FBI's New York Field Division in the criminal investigations related to the September 11th attacks.

FINE: Our review found that the FBI sometimes used these exigent letters in non-emergency circumstances. In addition, the FBI failed to ensure that there were authorized investigations to which the requests could be tied.

The exigent letters also inaccurately represented that the FBI had already requested subpoenas for the information when in fact it had not. The FBI also failed to ensure that NSLs were issued promptly to telephone companies after the exigent letters were sent.

Rather, in many instances, after obtaining records from the telephone companies, the FBI issued national security letters months after the fact to cover the information obtained.

We concluded that the FBI's use of these exigent letters inappropriately circumvented the requirements of the NSL statute and violated attorney general guidelines and FBI policies.

In response to our report, we believe that the department and the FBI are taking our findings seriously. The FBI concurred with all our recommendations and the department's National Security Division will be actively engaged in oversight of the FBI's use of NSLs.

In addition, the FBI's Inspection Division has initiated audits of a sample of NSLs issued by each of its 56 field offices.

The FBI is also conducting a special investigation on the use of exigent letters to determine how and why the problems occurred.

The OIG will continue to review the FBI's use of national security letters. In addition to issuing a second report on the use of NSLs in 2006, we intend to monitor the actions that the FBI and the department are taking to address the problems we found in that review.

Finally, I want to note that the FBI and the department cooperated fully with our reviews, agreed to declassify information in the report, and appear to be committed to addressing the problems we identified.

We believe that significant efforts are necessary to ensure that the FBI's use of national security letters is conducted

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

in full accord with the statutes, attorney general guidelines and FBI policy.

That concludes my testimony. And I would be pleased to answer any questions.

CONYERS: Thank you, Attorney General (sic).

Will the person in the back row standing up please sit down or leave this committee room?

I'm now pleased to welcome the general counsel for the Federal Bureau of Investigation, Ms. Valerie Caproni.

CAPRONI: Thank you.

Good morning, Mr. Chairman, Ranking Member Smith and members of the committee.

It's my pleasure to appear before you today to discuss the recent report by the Department of Justice Office of Inspector General regarding the FBI's use of national security letters.

I've submitted a detailed written statement, and, in the interest of time, will stress only a few points.

The I.G.'s report is a fair report that acknowledges the importance of national security letters to the ability of the FBI to keep the country safe and the difficult environment in which our employees have been working since 9/11.

The I.G. found no deliberate or intentional misuse of the national security letter authorities, A.G. guidelines or FBI policy. Nevertheless, the I.G. review identified several areas of inadequate auditing and oversight of these vital investigative tools, as well as processes that were simply inappropriate.

The FBI fully supports each of the I.G.'s recommendations and have implemented other remedial steps not proposed by the I.G. Collectively, these reforms will ensure full compliance with both the letter and the spirit of the law.

NSLs generally permit us to obtain the basic building blocks of an investigation from third-party businesses. Unlike grand jury subpoenas used in criminal cases, however, national security letter authority comes from several distinct statutes and they have very specific rules that accompany them.

The NSL authority used most frequently by the FBI is that provided by the Electronic Communications Privacy Act, or ECPA. Through an ECPA NSL, the FBI can obtain subscriber information for telephones and electronic communications. It can obtain toll billing information and electronic communication transaction records.

Significantly, the FBI cannot obtain the content of communications through an ECPA NSL. That requires a court order.

ECPA NSLs are by far the most common NSL that we use.

CAPRONI: Pursuant to the Right to Financial Privacy Act and the Fair Credit Reporting Act, we also have the authority to issue different types of national security letters.

The authority to issue an NSL lies at a senior level within the FBI. It can only be issued by an official who ranks not lower than special agent in charge or deputy assistant director. All such officials are career government employees.

And before an NSL can be issued, such employees must certify that the information sought is relevant to an authorized national security investigation.

As directed by Congress, in connection with the I.G.'s report, we endeavor to declassify as much information as possible, in order to maximize the transparency of our use of this important national security tool.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

To that end, for the first time, the public has a real sense of the frequency with which the FBI uses national security letters.

In the period covered by the report, the number of NSL requests -- that's not letters; remember that one letter can have multiple requests -- has ranged from approximately 40,000 to 60,000 per year. And we have requested information on fewer than 20,000 persons per year.

For a variety of reasons that will be discussed below, those numbers are not exact. Nevertheless, for the first time, the public can get a sense of the order of magnitude of these requests.

There are three findings by the I.G. that were particularly disturbing to me, and it is those three findings that I wish to address at some length this morning: first, inaccurate reporting to Congress; second, the use of so-called exigent letters; and third, violations of law and policy with respect to the usage of NSLs.

I am particularly distressed by the fact that the I.G. found significant inaccuracies in the numbers that we report to Congress. The responsibility to gather the data for congressional reporting lies with my division, and we did not do an acceptable job. The processes we put in place for tabulating NSLs were inadequate, and we had no auditing process in place to catch errors.

Although we realized we had a problem prior to the I.G.'s report and we're working on a technological solution, that realization came later than it should have, and for that I bear responsibility.

CAPRONI: At some point several years before I arrived at the FBI, our process for congressional reporting shifted from a totally manual process to a stand-alone database. While the OGC database was a giant technological step forward from 3x5 index cards, it quickly became an unacceptable system given the increase in our use of national security letters since 9/11.

The OGC database is not electronically connected to ACS, the system from which we derive the data. Instead, there's a manual interface between ACS and the database: An OGC employee is responsible for taking every NSL lead that is sent to OGC and manually entering the information into our database.

Nearly a dozen fields must be manually entered, including the file number of the case in which the NSL was issued, which is typically at least 15 digits and letters.

Needless to say, human error creeps in.

Approximately a year ago, when we were unable to tick and tie numbers in the database to previously reported numbers, we recognized that our technology was woefully inadequate. We began at that point to develop an automated system to improve our ability to collect this data.

That system, in addition to improving data collection, will automatically prevent many of the errors in NSLs that we will discuss today by automating much of the work associated with preparing NSLs.

The system will also allow us to automatically ensure that required reporting data is accurately collected.

The NSL system is being designed so that the FBI employee requesting an NSL will enter data only once.

For example, an agent or analyst who wishes to get telephone toll billing records will only have to tell the system that he is seeking an ECPA NSL for toll records and type the telephone number once.

The system will then automatically populate the appropriate fields in the NSL and the authorizing electronic communication. The system will ensure that the two documents match exactly and will minimize the opportunity for transcription errors that gave rise to unauthorized collections.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

Agents and analysts will still be required to provide the narrative necessary to explain why the NSL is being sought, the factual basis for making a determination that the information is relevant to an appropriately predicated national security investigation, and the factual basis for any determination that the NSL should include a nondisclosure provision.

CAPRONI: We're optimistic that we'll be able to pilot the system this summer and roll it out to all the field offices by the end of the year. At that point, I will be much more confident that in the future the data we provide to Congress is as accurate as humanly possible.

In the meantime, we're taking several steps to correct the numbers we previously reported. We've discussed our methodology with the I.G. and we will offer him the opportunity to review our work. We're striving to have the corrected reports to Congress as soon as possible.

The next significant finding of the I.G. I would like to discuss this morning involved the use within one unit at headquarters of so-called exigent letters. These letters, which numbered in excess of 700, were provided to telephone companies with requests for toll billing information.

All of the letters stated that there were exigent circumstances. And many stated that federal grand jury subpoenas had been requested for the records, even though, in fact, no such requests for grand jury subpoenas has been made.

From an audit and internal control perspective, the FBI did not document the nature of the emergency circumstances, did not keep copies of all of the exigent letters it provided to telephone companies, and did not keep records to track whether it had subsequently provided further legal process.

Moreover, some employees told the I.G. that there was not always an emergency relating to the documents that were sought.

OGC has been working with the affected unit to attempt to reconcile the documentation and to ensure that any telephone record that we have in an FBI database was obtained because it was relevant to an authorized investigation and that appropriate legal process has now been provided.

If we are unable to determine the investigation to which a number relates, they will be removed from our database, and the records will be destroyed.

The I.G. rightfully objected to the FBI obtaining telephone records with a letter that stated that a federal grand jury subpoena had been requested when that was untrue. It's unclear why that happened.

The director has ordered a special inspection in order to better understand the full scope of internal control failures and to make sure that in fact every record obtained pursuant to a so-called exigent letter has been appropriately connected to a national security investigation.

That review will also determine whether the practice discussed by the I.G. existed anywhere other than in the headquarters unit identified in the report.

In response to the obvious internal control lapses this situation highlights, changes have already been made to ensure that this situation does not recur. Any agent who needs to obtain ECPA-protected records on an emergency basis must do so pursuant to 18 USC Section 2702. 2702 permits a carrier to provide information regarding its customers to the government if the provider believes in good faith that there is a life-or-death-type emergency that requires disclosure of the record.

By FBI policy, a request for disclosure pursuant to that provision generally must be in writing and must clearly state that the disclosure without legal process is at the provider's option.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

The emergency must also be documented to our files so that the use of the letter can be audited.

The policy allows for oral requests, but any oral requests have to be approved and documented to the file.

CAPRONI: The I.G. also examined misuse of NSLs that had been reported and some that had not as part of the IOB process. As this committee knows, pursuant to executive order, the president has an Intelligence Oversight Board that receives from the intelligence community reports of intelligence activities that the agency believes may have been unlawful or contrary to executive order or presidential directive.

The I.G. found that from 2003 to 2005 the FBI had self-reported 26 potential violations involving NSL authorities. The I.G. also found, however, a number of potential IOBs in the files it examined that had not been reported to OGC for adjudication.

Although press accounts of this report have implied that the I.G. found massive abuses of the NSL authorities, a careful read of the report does not bear out the headlines.

The I.G. examined 293 NSLs; a reasonably small, nonrandom sample. We do not suggest that the sample was not a fair sample, but only point out that it's questionable from a statistical standpoint to attempt to extrapolate from a very small sample to an entire population.

Of the 293 NSLs the I.G. examined, 22 were judged to have a potential unreported violation associated with them. Of that 7 percent, 10, or almost 50 percent of that group, were third-party errors; that is, the NSL recipient provided the FBI with information that we did not seek.

CAPRONI: Only 12 of the NSLs examined, or 4 percent of the total group, had mistakes that the I.G. rightfully attributes to the FBI.

Examining the 12 potential errors that were attributable to the FBI reveals a continuum of seriousness relative to the potential impact on individual rights.

Four of them, or just over 1 percent of the sample, were unquestionably serious violations. Specifically, two of the violations involved obtaining full credit reports in counterintelligence investigations, which is not statutorily authorized.

One involved issuing a national security letter when the authorization for the investigation to which it related had lapsed. And one involved issuing an NSL for information that was arguably content, and therefore not available pursuant to NSL.

The remaining eight potential errors involved lack of attention to detail, and did not involve the FBI seeking or obtaining any information to which it was not entitled.

We do not excuse lack of attention to detail. And I have admonished the lawyers in the field who review NSLs that they must be careful so that they can avoid this sort of error.

But we do believe that such mistakes pose different challenges and risks, in seeking information to which you are not entitled.

In short, approximately 1 percent of the NSLs examined by the I.G. had significant errors that were attributable to FBI actions and that had not been, but should have been, reported as potential IOB violations.

A 1 percent error rate is not acceptable, and we have taken steps to reduce it. Those steps are discussed at length in my written testimony, and I will not repeat them here.

But among the steps I do want to mention is the director's order to special inspection of all field officers' use of

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

national security letters, an inspection that began on Friday.

We offered to fully brief the committee on the results of that inspection when it is complete.

Several of the actions we are taking involve changes to FBI rules and policy.

Rules will, of course, only eliminate errors if they are followed. The I.G.'s report has painfully demonstrated for us that, while establishing policy -- that while we are good at establishing policy and setting rules, we are not as good as we must be at establishing internal controls and auditing functions to make sure that the rules are followed.

CAPRONI: The full parameters of an FBI-compliant program have not been set, and the inspection that is currently under way will clearly influence the parameters of the program.

In short order, however, the FBI will establish a vigorous multidisciplinary compliance program that assures as well as any compliance program can that our employees faithfully adhere to all of rules and policies, particularly those that are designed to protect privacy and civil liberties.

The FBI is acutely aware that the only way we can achieve our mission of keeping the country safe is if we are trusted by all segments of the American public.

With events like the London terror attack of two years ago, we were all worried about the risk of a catastrophic attack from homegrown terrorists. Our single best defense against such an attack is the eyes and ears of all Americans, but particularly in those segments of the population in which the risk of radicalization is at its highest.

We need people in those communities to call us when they hear or see something that looks a mess. We know that we reduce the probability of that call immeasurably if we lose the confidence of any part of the American public.

CONYERS: Counsel, can you wind down at this point?

CAPRONI: Yes, sir.

CONYERS: All right.

CAPRONI: We will put into place a compliance program to maximize the probability that we do not lose the confidence of the American public by dint of the sort of errors highlighted in this report.

I appreciate the opportunity to appear before the committee and look forward to answering your questions. Thank you.

CONYERS: Well, General Counsel Caproni, I want to thank you for your candor and forthcomingness in coming before us today. And we will include the rest of your testimony, of course.

CONYERS: Now, let me begin the questioning. And I thank both the witnesses.

Mr. Inspector General Fine, I'm curious as to how you've come to the conclusion that these errors that have been reported and that bring us to this chamber were either sloppy -- the results of sloppy book-keeping, recordkeeping or compliance with the law, but none of it was intentional.

How could that be if they've known about these excesses since the year 2004, their communications analysts unit warned them about it in early 2005, and we have something like at least over 700 exigent letters and somewhere in the neighborhood of 40,000 to 50,000 NSL letters for three years?

FINE: Let me separate some of those issues.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

I don't believe that they intended to go out and obtain information that they knew they could not obtain and said, "We're going to do it anyway."

I think what they did was complete carelessness, did not follow the rules, did not follow appropriate procedures, and obtained information that they could have obtained properly but by taking shortcuts.

Now, we didn't do a review to ask everybody what was in their mind and what exactly they did. But we saw instances where people just simply didn't follow the rules and didn't take appropriate action.

CONYERS: But they were being warned.

FINE: Yes.

CONYERS: This didn't just come up recently. This goes back to 2004.

FINE: In 2004, it is correct that attorneys in the Office of General Counsel had concerns about the exigent letters and weren't saying, "Stop it," but were saying, "We need to take different measures to issue these letters."

CONYERS: Do you think that the law was so complicated that people in good faith just couldn't figure out what it was we were requiring?

FINE: I think what they did was inappropriately take a model from another context and applied it to this context, which was wrong, it clearly was, and that they did not think carefully and they did not take appropriate actions.

Now, I know that the FBI is conducting a special inspection to look exactly at what everybody knew and when they knew it and why they took the actions that they did.

We didn't do that kind of review. We didn't ask everybody up and down the line. And it is possible that people had motivations that were inappropriate.

CONYERS: There's no way we can tell. There's no way I can tell, but there's no way you can tell either.

FINE: It is true that we did not do a performance review of every individual. So I think that's an appropriate point, Mr. Chairman, I really do.

And I do think it's incumbent upon the FBI to go back and look and see exactly what people were doing, at what stages, and why they did what they did, and take appropriate action to hold people accountable.

CONYERS: Now, do you make a distinction between the national security letters and the exigent letters in terms of the severity of the offense that brings us here today?

FINE: I do. I think the exigent letters were the most troubling aspect of this.

CONYERS: And why is that?

FINE: Because there's a process in the law to allow voluntary disclosures from these telephone companies if there is a true emergency. And we believe the FBI should have followed that voluntary process.

Instead, they went with these exigent letters, which they use in a different context, and applied it to this context, which, in our view, was inappropriate.

With regard to the national security letters, there were many of them, and many of them did comply with the requirements of the law we saw. And we tried to do a review to see how many didn't. We found a significant number didn't.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

But with regard to the exigent letters as a whole, that whole practice was very troubling to us in and of itself.

CONYERS: Now, are you satisfied with the steps that have been described here today by the general counsel in terms of how we clean this mess up?

FINE: Well, we have been briefed by the department and the FBI about the steps they're taking. I think they are taking this seriously. But I'm not in a position right now to say, "I'm completely satisfied, I trust all this."

We need to see what happens with these steps, see whether they're concerted efforts over time, to see whether they really are adequately implemented.

So I can't say right now that it is -- they've done all they can.

FINE: But I think they are taking important steps and taking this very seriously.

CONYERS: All right. Thank you so much.

And I recognize Lamar Smith.

SMITH: Thank you, Mr. Chairman.

Mr. Chairman, I'm hoping my first question won't count against my time.

Mr. Fine, I noticed in reading your bio that when you were a senior in college and co-captain of the basketball team, you were recruited by the San Antonio Spurs. They happen to be my hometown team.

My question is this: Don't you regret not playing for the Spurs...

(LAUGHTER)

... rather than becoming a Rhodes scholar and graduating from Harvard Law School?

CONYERS: The gentleman's time has expired.

(LAUGHTER)

FINE: Congressman, I was drafted in the 10th round by the San Antonio Spurs. And if I was maybe a little taller than 5'9", I might have had a chance to play.

So I don't really regret that my future was in the law, rather than professional basketball.

But I tell people who don't believe I actually played basketball when they see me at 5'9", before I started this job as the I.G., I was 6'9".

(LAUGHTER)

SMITH: Very good answer.

Mr. Fine and Ms. Caproni, let me address a more serious question to both of you all, and it is this: We've unearthed these problems that are recognized and that are being dealt with. And some of the reasons for those problems have already been seen and the practice has been discontinued.

But my question is this: Do you all feel that the problem is with how the law was enforced rather than with the law itself? In other words, if the law were carried out as intended, doesn't that solve our problem?

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

Mr. Fine, first.

FINE: You know, Congressman, I'm really not in a position to say what the law should be or if there should be modifications to the law.

My job is to look at the law and look at the application of the law and see the problems that occurred.

I do believe that if the FBI had assiduously and carefully applied the law, we wouldn't have seen as many problems as we have. And it really was unacceptable and inexcusable what happened here.

SMITH: Ms. Caproni?

CAPRONI: From our perspective, the problem is not with the law. Although, I would note that unlike other areas that our agents -- where they get these sorts of records, there are very specific rules and they have to wend through those rules. That, in my sense, is our responsibility as the lawyers to make sure that the agents understand what they can do and what they can't do.

CAPRONI: Again, there is no doubt that the problem with the national security letters was a colossal failure on our part to have adequate internal controls and compliance programs in place.

The laws themselves provide us with a needed tool. And it's a tool that we should use responsibly.

SMITH: OK, thank you.

Mr. Fine, Ms. Caproni, why are national letters of security -- national security letters important in our investigation of terrorism?

CAPRONI: They are critical. They are -- national security letters provide us the basic building blocks that we need to build an investigation.

For those of you who had prior criminal AUSA experience -- and I know a number of you did -- you're used to issuing grand jury subpoenas to provide -- to obtain telephone records and banking records.

Frequently, in terrorism investigations, we don't have an open criminal investigation.

In fact, that was one of the things that the 9/11 Commission really encouraged us to do, and this committee encouraged us to do, and the intelligence committees, to move more -- when we're thinking about terrorism case, move from simply a criminal mindset to thinking in intelligence mindset.

So a national security letter is the tool that we use in order to get the basic building blocks of those investigations: again, like phone records for almost every terrorism, financial records when we're building terrorism financing cases.

So without national security letters, our national security investigations would really be stopped before they even got started.

SMITH: OK, thank you.

Mr. Fine?

FINE: I do think that they are important investigative tools. They can connect terrorist individuals with terrorist groups. They can find out where terrorist financing can occur. They're indispensable in counterintelligence investigations. And the FBI did tell us, from folks in the field to headquarters, how important they were to the investigations, and showed us examples of that.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

Having said that I think they're important, there needs to be important checks on these tools because they are obtrusive, and there is information that is obtained and retained for significant periods of time.

And so, while they are important investigative tools, there also needs to be appropriate checks on them as well.

SMITH: Mr. Fine, in your conclusions -- it's the second one -- you say, "In most but not all of the cases we examined in this review, the FBI was seeking information that it could have obtained properly through national security letters."

SMITH: What percentage would you guess is that? In other words, what percentage of the problems could have been resolved if they had obtained national security letters?

FINE: We found instances -- a few instances where they obtained information inappropriately and could not have used a national...

SMITH: How many of the 739 would you guess that is?

FINE: Well, the 739 is hard to tell, because they could not tie them to appropriate investigations all the time; and there were many times where they couldn't tell if it was an emergency. So I don't know how many in the 739. That's the most troubling aspect of it.

With regard to the others, the national security letters and the files we reviewed, I'd say we found about seven where there were illegal uses of them where it was attempting to obtain information through confusion, through error, information that they were not entitled to obtain through a national security letter -- either an educational record or obtaining information -- a full credit report in a counterintelligence case, which they're not allowed to obtain; or not using an NSL.

SMITH: You said seven times?

FINE: Seven of the ones that we found. And we found in our -- well, seven of the individual ones. And, as you recall, we didn't do a review of every NSL that was issued. We did a small sample of them.

SMITH: OK. Thank you, Mr. Fine.

Thank you, Mr. Chairman.

CONYERS: Thank you very much.

The gentleman from New York, Jerry Nadler?

NADLER: Thank you.

Ms. -- well, Mr. Fine, I suppose: You stated in your report that there were no intentional violations of NSL policy procedure; that these were basically carelessness, but there were no intentional violations. No crimes.

FINE: Correct.

NADLER: OK.

But we also read in the report that agents intentionally went around the statute to provide phony information requests to telephone companies based on false statements. For example, the FBI's Communications Analysis Unit went around the NSL statute because it felt that the statute was insufficient, and contracted with the telephone companies to access information directly.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

These contracts were approved by the Office of General Counsel and exploited by issuing exigent or emergency letters which -- well, let me ask the general counsel.

What is the statutory basis for an exigent letter? As far as I can tell, there is no basis for it.

CAPRONI: Well, under 2702, we have the authority to get records from a phone company in an emergency circumstance without a national security letter.

The exigent letters were undoubtedly an inappropriate shortcut to the process, though.

NADLER: Well, under 2702, if you were going to get information in an emergency, what do you have to do?

CAPRONI: You simply have to tell the carrier that there's an emergency, explain -- we recommend that you explain to the carrier what the emergency is.

CAPRONI: And it's then up to the carrier to decide whether or not to provide us records.

So it's not a compulsive system.

NADLER: It's not a compulsive. But, of course, the carrier has no particular interest in protecting -- if you're looking at my records or you want my records, for example, the phone company has no particular interest in protecting my privacy rights, and I never find out about it, so I can't go to court to protect them. Correct?

CAPRONI: I don't represent the carriers, but I would disagree with the theory that they have no particular interest in protecting your records. In fact...

NADLER: What is their interest?

CAPRONI: In fact, the carriers were diligent in making sure that any record they gave to us they subsequently obtained a national security letter for.

NADLER: But wait a minute. But Mr. Fine's report says that in many, many instances, hundreds of instances, that never happened.

CAPRONI: As of right now there are still some numbers that have not received national security letters to back up the requests.

NADLER: Well, back up years later after the report. But that's backfilling. In other words -- and that's certainly not evidence that the phone companies were diligent in seeking these things. That's saying that after this report was done someone said, "Wow, we got a problem on our hands. We better go get these letters four years later, or three years later." So that's not evidence of what we're talking about.

CAPRONI: Respectfully, even though I'm not defending their practice, it is not the case that it was only after Mr. Fine's report came out that they were attempting to make sure that the paperwork documentation was appropriate for every record they obtained.

And let me also say...

NADLER: And you think the paperwork documentation should be done and appropriate.

CAPRONI: And if it's not, the records are going to come out of our database and be destroyed.

NADLER: And in this morning's Washington Post it says, "Under past procedures, agents sent exigent circumstances letters to phone companies seeking toll records by asserting there was an emergency. Then they were

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

expected to issue a grand jury subpoena or national security letter which legally authorized the collection after the fact. Agents often did not follow up with that paperwork, the inspector general's investigation found." That we know.

The new instructions -- which according to The Washington Post were just issued to the FBI -- tell agents there is no need to follow up with national security letters or subpoenas. The agents are also told that the new letter template is the preferred method -- preferred method in emergencies, but that they may make requests orally, with no paperwork sent to phone companies.

So in other words, it appears from this morning's Washington Post that instructions are now being given to the FBI not to bother with any backup documentation after an oral request to the phone companies for records invading people's privacy.

CAPRONI: No. Quite the contrary.

The instructions are that if they get information based on an oral request -- and just to give an example of why that -- when that might be appropriate. If a child has been kidnapped and the ransom call comes in...

(CROSSTALK)

NADLER: Oh, I don't -- obviously, in those -- I'm not questioning the need in an emergency like that for getting records right away. Obviously.

(CROSSTALK)

CAPRONI: ... get them on an oral request.

NADLER: I don't doubt it.

What I'm questioning is that, according to today's Washington Post, the opposite of what the two of you are saying is the case and that now they seem to be saying, "Well, we'll take care of this lack of follow-up by documentation by simply declaring it unnecessary."

CAPRONI: No, Congressman, that's not the policy.

The policy now is that if a request is going to be made on an emergency basis for records, that has to be documented. It has to be documented in the first instance in the request. But if there is not time to do that so that you need an oral request, then that has to be documented to the file, together with the approval for it.

So it is, again, an internal control to avoid the problem that was existing in CAU, which was "emergency" had become a flexible term...

NADLER: OK. And I have one final question, and that is to Mr. Fine, just a quick clarification on accessibility of PIN numbers and Social Security numbers of individuals through this process.

On page 73 of your report, there's a discussion of a potential intelligence review board violation because an agent accessed a bank balance by getting a person's bank account and PIN number from the result of a FISA order.

The agent was faulted for not using an NSL, but was not faulted for the fact that the PIN number was readily available.

And the reason I flagged this, because this reference makes clear that through an NSL or a 215 order the government can secretly obtain the PIN number for someone's credit or debit account along with their account number and all their identification.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

CONYERS: The gentleman's time has expired.

Finish.

NADLER: Well, what limits are there on this and what protections are there on this power to get PIN numbers and credit account numbers?

FINE: The FBI can get bank records and records like that. There has to be predication for it, and they have to show the need for that.

And that is one of the tools that the FBI has used and can use. And as we pointed out, that's one of the reasons there need to be controls on this.

CONYERS: The gentleman's time has expired.

The chair turns to the former chairman, Jim Sensenbrenner from Wisconsin, whose letter to the Department of Justice first triggered the inquiries that have flown from this. And I congratulate him and recognize him at this time.

SENSENBRENNER: Well, thank you very much, Mr. Chairman.

Just by way of background, we did some oversight when I was the chair of the committee, and received a letter in late 2005 that indicated that there were problems with national security letters. And the audit that the inspector general conducted was as a result of a provision that I put in the Patriot Act reauthorization that required this audit to be made, as well as the subsequent audit that Mr. Fine is doing that I'm sure we're going to talk about extensively later when the report is issued.

I'd also like to point out that national security letters were not authorized by the initial Patriot Act in 2001, but have been around since 1986 in legislation that was authored by Senator Patrick Leahy of Vermont, who is the chairman of the Judiciary Committee on the other side of the Capitol.

The Patriot Act reauthorization put in a number of civil liberties protections relative to national security letters because we knew that there were problems afoot and decided that even though NSLs were not a part of the Patriot Act, that they needed to have civil liberties protections.

And I am proud of that work that this committee did, and eventually found its ways into the Patriot Act reauthorization act which was signed by the president in March of last year.

One of the things, Ms. Caproni, that I am really concerned about is that the Justice Department, and the FBI in particular, have come to the Congress repeatedly over the last dozen years asking for administrative subpoena authority, meaning that subpoenas could be issued without judicial supervision.

SENSENBRENNER: This Congress has repeatedly rejected each and every one of those requests.

Now, a national security letter is kind of like an administrative subpoena, although it is limited to the type of information that can be obtained.

I'd like to know from both of the witnesses whether the FBI simply turned around and used NSLs to get huge amounts of information, after Congress said no again to administrative subpoena authority.

CAPRONI: No, we didn't.

National security letters are always focused on a particular case. There's no bulk collection via national security letters.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

And while our congressional reporting numbers are off, as Mr. Fine correctly found, they are not off by an order of magnitude. That is, that we reported that we collected data on less than 20,000 people a year. While that number may go up, it's not going to go up to above, you know, 200,000.

SENSENBRENNER: And how can you account for the fact that the number of NSLs that were issued before 9/11 was about 8,000-plus per year, and then it went up to 150,000?

CAPRONI: I think there are...

SENSENBRENNER: Do we have that many potential terrorists running around the country? If so, I'm really worried.

CAPRONI: I think it's a function of two things.

(CROSSTALK)

CAPRONI: First off, I think it's a function of the fact that, post-9/11, a number of agents were moved into the counterterrorism area and the director directed that no lead in a counterterrorism case would go unpursued.

So there is a directive to agents that they must cover all counterterrorism leads. That's point one.

But I think point two was, because we were focusing much more on an intelligence-driven reaction to counterterrorism threats, the toolbox that we were using was focusing mostly on national security letters, as opposed to the prior reaction, which would have used grand jury subpoenas to get the same records.

SENSENBRENNER: OK.

Mr. Fine?

FINE: I agree with Ms. Caproni. Prior to the September 11th attacks, it was rarely used. There were delays in getting them, and they were not following the leads that they would have followed after the 9/11 attacks.

FINE: After the 9/11 attacks, they were attempting to connect the dots, they were attempting to track down leads. When there are indications from a terrorists overseas that there might be connections to the United States, they try and follow it.

SENSENBRENNER: My time is running out.

You know, I just make the observation that one of the things that gets people in this town in big trouble is overreaching.

I think that, given your report, Mr. Fine, the FBI has had a gross overreach. What this does is it erodes support for the function that the FBI does to protect all of us from future terrorist attacks.

You know, I hope that this would be a lesson to the FBI that they can't get away with this and expect to maintain public support for the tools that they need to combat terrorism.

Given the way the FBI has acted, I have my doubts. But let this be a warning.

And my time is up.

CONYERS: The chair recognizes the gentleman from Virginia, Bobby Scott.

SCOTT: Thank you, Mr. Chairman.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

Mr. Fine, you've suggested that there's some confusion in how to work these things. There were, as I understand it, representations that there was an emergency when, in fact, there was no emergency; and representations at grand jury subpoenas had been issued when, in fact, they had not been issued.

SCOTT: Is that right?

FINE: That is correct.

SCOTT: Has anyone been sanctioned?

FINE: No, the FBI, as a result of this report, is going and looking at -- a special inspection to look at exactly what happened with this, how the problems occurred and to determine accountability. And I think that is appropriate.

SCOTT: To your knowledge no one has been sanctioned so far.

FINE: Not yet, no.

SCOTT: OK.

Ms. Caproni, you indicated that we need to change our mindset from criminal investigation to intelligence gathering.

CAPRONI: I'm saying that post-9/11 that's been what the FBI has been charged with doing, is really not thinking of our terrorism investigations as wholly criminal.

SCOTT: OK, now, when we use these letters, are we obtaining information regarding United States citizens?

CAPRONI: Sometimes.

SCOTT: That's a yes?

CAPRONI: The national security letters...

SCOTT: Not always, but sometimes.

CAPRONI: Right, it's about half and half.

SCOTT: You're using this mindset against United States citizens.

OK, when you get all this information, like Social Security numbers and phone records, how long is this information retained?

CAPRONI: The issue of retaining national security -- data that's obtained via national security letters is subject to a working group that the DNI is chairing together with the Department of Justice and that we will participate on in terms of how long we should keep it.

As of right now, it's subject to the normal archive rules, and so we keep it for whatever the law under archives requires, which is typically 20 years.

SCOTT: Twenty years.

Now, how many criminal convictions have you gotten from NSL letters, information -- how much information from NSL letters has resulted in criminal convictions for terrorism-related offenses?

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

CAPRONI: That was one of the questions that the I.G. was charged with answering. And I think deriving it is very difficult, because while national security letters are typically used in the beginning of an investigation, we don't tag the data, and so tracing it through to know whether national security data started in a case that ended in an investigation.

SCOTT: Well, Mr. Fine, can you answer the question?

FINE: No, we tried to, but you cannot tell how many convictions resulted. It's not specifically segregated or tagged or tied. And when we tried to follow it through the system, it was very hard to do that. So I can't give you a number.

SCOTT: If somebody said one, would that surprise you? Could you contest that number?

CAPRONI: I would.

FINE: I would think it would be higher, but I can't tell you one way or the other.

SCOTT: What information is obtained through NSL letters that could not have been gotten through going through the normal FISA process, even in emergencies, when there's an after-the-fact process with the FISA Courts?

CAPRONI: Anything that we can obtain through a national security letter could be obtained from a FISA 215 order.

I would tell this committee that I think if you changed the law in that way, you would be doing grave disservice.

CAPRONI: It would essentially sink the system.

We issue, as you can tell from the report, thousands of national security letters to get information. We do not have an infrastructure in place to take every one of those to court any more than an AUSA in any district has the infrastructure in place to go to court to get every grand jury subpoena.

It's simply not -- we don't have the infrastructure to do that.

SCOTT: So you're not getting any information you couldn't get through FISA but just administratively...

CAPRONI: Well, the Patriot Act...

SCOTT: You would have a judge looking at what you're doing and not having a process that lacks oversight?

CAPRONI: Congressman, under the FISA statute, Section 215 of the Patriot Act gave us the authority to get an order for any type of record.

SCOTT: Well, that's what we're talking about.

Mr. Fine, did I understand that in these cases there's an actual ongoing investigation prior to issuing these letters, or there's not an identifiable investigation ongoing when they issue the letters?

FINE: It has to be tied to some investigative file. They have to open an investigative file or a threat assessment or preliminary inquiry, a full inquiry. It has to be tied to one of those. It can't be issued out of a control file.

SCOTT: That's what they're supposed to do. Are they doing that?

FINE: We found that there were instances where they didn't; that they were issued out of control files and they were not tied to a specific investigation.

SCOTT: Well, if there's no ongoing investigation, what is the standard for deciding when to issue one and when

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

not?

CAPRONI: The standard is that it has to be relevant to an authorized investigation.

What Mr. Fine was talking about with the control files is, while it's a difficult situation to understand, those NSLs were -- in fact, they related to an authorized investigation. There was a bureaucratic problem, which nobody likes to hear that it's a bureaucratic problem that we believe we have worked out.

None of the NSLs that were issued out of control files did not relate to an authorized investigation. They all were tied to investigations that were appropriately opened.

CONYERS: The distinguished gentleman from North Carolina, Howard Coble?

COBLE: I thank the chairman.

And good to have you all with us.

Mr. Fine, your report recommends a number of changes on the FBI's use and tracking of national security letters. The attorney general issued a press release on March 9th responding to those recommendations.

COBLE: And I presume each of you is familiar with that report -- are you not? -- the March 9th report.

Let me put this question to each of you: Will those recommendations submitted by the A.G. restore the FBI's accountability for its use of NSLs?

Mr. Fine, let me start with you.

FINE: I believe that the response to the recommendations and what the FBI and department is doing is appropriate.

Is it sufficient? Is it all that needs to be done? I'm not sure. We'll have to see what the results of those steps are.

We tried to provide recommendations to ensure that these very important but sensitive tools are used in full accord with national security letter authorities, with A.G. guidelines and internal control policies.

They hadn't been in the past. We'll have to see if they are now.

COBLE: Ms. Caproni?

CAPRONI: I think we're going to have to work to get the trust of this committee back. And we know that that's what we have to do, and we're going to do it.

COBLE: Let me ask you this, Ms. Caproni: Can the FBI implement the attorney general's directions within the four months when the A.G. has requested Mr. Fine to report on your progress?

CAPRONI: I hope so. There's some that are going to require some, sort of, interagency work. But, certainly, we will -- if not, all of them will be fully implemented in four months since we will have made substantial progress.

COBLE: And you may have address this earlier, Ms. Caproni, but let me put it to you in case you did not: Does the FBI have any discrepancy or challenge with the report that Mr. Fine has issued?

CAPRONI: No. We accept the report. To the extent we had factual quarrels, we worked those out and either we persuaded them or they persuaded us.

COBLE: What do you think -- you may not be able to respond to this -- what do you think, Ms. Caproni, are the

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

greatest obstacles that your office faces in implementing the A.G.'s directions?

CAPRONI: I think that any obstacles there are, the director is going to make sure are removed. I think it's time, it's energy and effort, and we're going to do it.

COBLE: I thank you both for being here.

Mr. Chairman, if I may, I would like to submit for the record the March 9th press release submitted by the attorney general.

CONYERS: Without objection, so ordered.

COBLE: And I thank the chairman, and I yield back my time.

CONYERS: The other gentleman from...

PROTESTER: (OFF-MIKE) not any of these FBI (OFF-MIKE)

CONYERS: I ask the lady to -- no, don't sit down now. I ask you to please excuse yourself from this hearing. No visitors can interrupt a hearing in the Congress.

PROTESTER: (OFF-MIKE)

CONYERS: Just a moment.

Would the officers escort this lady out please?

The chair recognizes the other distinguished member from North Carolina, Mr. Mel Watt.

WATT: Thank you, Mr. Chairman. And I thank the chairman for convening the hearing.

Mr. Fine, I'm looking on page seven of your testimony in which you indicate that you reviewed 293 national security letters in 77 files and found 22 possible violations that had not been identified or reported by the FBI.

WATT: And I'm trying to extrapolate that, although Ms. Caproni seemed to take some issue with whether that was a reliable sample.

I'm trying to assume for the moment that it is, without trying to figure out how many there would be of the total national security letters that were possible violations.

My formula is I'm starting with 143,000 national security letter requests, on page five. Would that be an appropriate place to start? Or have you done the extrapolation for me?

FINE: I haven't done it, but there are 143,000 requests. And, as you know, a request -- there can be multiple requests in a letter. So there are approximately 45,000 letters during the time period, with 143,000 requests.

So I think the starting point would be about 44,000 letters during the time period.

WATT: And if you extrapolated the possible violations out, what would that come to, according to your math?

FINE: If you're talking about 7 percent, approximately 7 percent of the 293 had a violation. So 7 percent of 44,000 would approximately be about 3,000.

WATT: So you're telling me...

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

FINE: That's quick math; I hope that's correct, but I think it is.

WATT: It is possible that my FBI and my people who are supposed to be protecting my interests violated the law how many times?

FINE: Well, I think there are possible violations of either the law, the attorney general guidelines or the FBI's policies several thousand times if you statistically extrapolate. It was a small sample.

FINE: We didn't think it was skewed or biased. But if it held up for the entire population of files, several thousand; some more serious than others, but that's a lot.

WATT: Ms. Caproni, why ought not our public be concerned about that kind of disregard of the law and internal process?

CAPRONI: Well, I think the public should be concerned. We're concerned. And we're going to fix it.

I would say, as Mr. Fine said, the sort of errors range, sort of, on a long continuum of seriousness. The most serious errors that Mr. Fine identified were obtaining full credit reports in counterintelligence cases.

We have had a concerted effort to find all such errors.

WATT: That's seven of the 22 files, where you say they were real serious violations.

Extrapolate that out for me, Mr. Fine.

CAPRONI: That -- 1 percent...

FINE: Well, I think, in Ms. Caproni's testimony, she talked about how -- the level of seriousness and which were FBI errors and which were company errors, and came up with the figure that about 1, a little bit over 1 percent of them were serious violations involving FBI errors.

If you extrapolate that to the entire population, that would be about 600 cases of serious FBI misconduct.

WATT: Ms. Caproni, is there some reason that this committee and the American public shouldn't be concerned about law enforcement violating the law...

CAPRONI: Again, we are...

WATT: ... 600 times?

CAPRONI: We are quite concerned about this, Congressman. And we are making every effort to figure out where those errors are, to sequester the material to pull it out of our files, and to destroy it.

We will also take appropriate action...

WATT: How many files have you all destroyed, based on this investigation, up to this point?

CAPRONI: When we identified data that we have...

WATT: Isn't that a number, rather than an explanation?

CAPRONI: Congressman, I don't know the number. I know that, when we identified data, we have...

WATT: Has the FBI destroyed any files, up to this point, based on this investigation?

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

CAPRONI: We destroy data all the time, when we discover it was improperly collected. So, both outside of Mr. Fine's investigation and he...

WATT: Have you destroyed any files based on this investigation?

CAPRONI: Again...

WATT: Have you destroyed any files based on this investigation?

CAPRONI: Not a file -- not a file, but we...

WATT: Have you destroyed any information based on this investigation?

CAPRONI: Yes.

WATT: What have you destroyed?

CAPRONI: The destruction would have been of the full credit reports that were obtained improperly. And I think there was also some telephone...

WATT: How many is that, Ms. Caproni?

CAPRONI: It's not much. It's -- but this process is going forward.

WATT: In these 600 cases that you've identified as possible real serious areas, or several hundred, have -- you intend to prosecute anybody for violating the law?

CAPRONI: We'll have to look at what the facts are. I'm not going to prejudge what the inspection...

WATT: How long is it going to take you to look at that?

CONYERS: The gentleman's time has expired.

CAPRONI: The inspectors are in the field now, and I think that they will have completed their inspection visit, which is a sampling process, but that we anticipate that they'll have completed it within a week or so.

WATT: You've got a more reliable sampling process than Mr. Fine...

CAPRONI: No, it's just bigger. It's bigger and it's across all field offices.

WATT: Thank you.

CONYERS: The gentleman from California wants an attorney general for his state.

(LAUGHTER)

Dan Lungren?

LUNGREN: Thank you very much, Mr. Chairman.

Ms. Caproni, I was one of the ones who have defended the FBI and the Justice Department in the use of these as we went through legislation the last two years. And to say that I'm disappointed doesn't give justice to what I feel about this.

Mr. Fine has said that this is the result of mistakes, carelessness, confusion, sloppiness, lack of training, lack of

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

adequate guidance, and lack of adequate oversight. That sounds like a report about a first or second grade class.

We're talking about agents of the FBI who are lawyers in many cases, who have college degrees, who have other kinds of education. We're talking about people who have gone through the FBI Academy. We're talking about people who presumably have been trained to go into this. We are how many years past 9/11?

And in response to the question, I believe it was of Mr. -- well, I'm not sure who asked you this, but whether you could get this done in four months, you said you hoped so.

I hope you'll deliver a message that we expect it will be done. I mean, because I don't think if you can't get it done in four months you're going to have to worry about improving your procedures for NSLs, because you probably won't have NSL authority.

I just -- I just want to convey to you how upset many of are who have defended this program and have believe it is necessary to the protection of our country. And you, the FBI, have an obligation, yes, to try and find out who the potential terrorists are, but also to make good on the promise we made to the people of America that the terrorists are not going to succeed by indirection what they can't do by direction, that is destroy the Constitution.

LUNGREN: And I just -- I'll tell you this, I talked with Mr. Mueller yesterday -- because I've known him for 30 years. He's "Mr. Fix It." He goes in and fixes messes. He's done it all over this government. I've seen his work in San Francisco. I've seen his work here at the Department of Justice.

If I didn't know him, if I didn't know his record, if I didn't know he's the man we put in many places to fix things, I would have no confidence in the FBI right now.

So I hope you'll deliver a message to all your people that it's not good enough to tell us you hope it's going to be done in four months. I hope you're going to deliver a message that it better be done in four months or you're not going to have NSLs to worry about.

And I say that as someone who supports him and will fight on the floor to have that authority given to you if there is proper oversight, but I probably won't get a majority of votes on the House floor if you don't fix it.

So can you tell me you're going to do better than you hope to fix it in four months?

CAPRONI: Congressman, you're absolutely right. Yes, it will be done.

LUNGREN: I appreciate that.

Now, Mr. Fine, you're the inspector general for the FBI. I want to congratulate you on what you've done. We say -- we take some satisfaction in your carrying out the authority we gave you, but sometimes that doesn't happen. And we appreciate the job you have done here.

But maybe you won't want to answer this question. Maybe you can help me: How do you explain carelessness, confusion, sloppiness, lack of training, lack of adequate guidance and lack of adequate oversight with the FBI?

I just turned on the television last night and watched one or two or three of these shows that always shows the FBI as being far better than local government -- that little burr under my saddle, because I'm a former A.G. of California. I appreciate the FBI, but how do you explain this?

I'm not sure what would be worse, frankly. At first I was relieved that you said this: "And it wasn't intentional action by the FBI." At least we haven't found that.

I would at first been more worried about that.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

LUNGREN: Now, as I think about this, should I be more worried about the fact that the FBI now, in something as important as NSLs, has marks of carelessness, confusion, sloppiness, lack of training, lack of adequate guidance and lack of adequate oversight?

Is this exceptional in your experience, in your oversight of the FBI?

FINE: I think the FBI worked hard to get these authorities, but didn't take it seriously enough putting in controls over these authorities. And I think there is often a problem sort of between the receipt of the authority and the execution of that authority. And that's clearly what happened here. And we were very troubled by it.

We've seen problems in the FBI in terms of information technology. In trying to upgrade their information technology we've seen problems. But these are difficult tasks and they are trying to do this as they're changing their mission.

And, quite honestly, there really is no excuse for it. There is no excuse for it.

LUNGREN: Did you have any question that the NSLs are of some value?

FINE: Yes, I do believe they're of value.

LUNGREN: And that if we lost them, that would be a loss?

FINE: I believe that they're a valuable investigative tool that are indispensable in many cases to counterterrorism and counterintelligence investigations. And that's why it is so troubling that they didn't...

LUNGREN: So we better fix this so we don't lose a tool that's truly effective?

FINE: I think they need to fix it.

LUNGREN: Thank you.

Thank you, Mr. Chairman.

CONYERS: The gentlelady from Houston, Texas, Sheila Jackson-Lee.

JACKSON-LEE: Again, Mr. Chairman, my appreciation for your continuing effort of establishing transparency in government.

I welcome both of the witnesses here today and recount just a limited history that troubles me as we find ourselves here today.

I know the good intentions of the witnesses, but certainly I'd need not remind you of the era of McCarthyism and certainly the role that law enforcement played in that misdirected era of the United States of America.

As a young lawyer, I participated in the investigations into the assassination of Dr. Martin Luther King and John F. Kennedy right here in this Congress. And what was exposed was the extensiveness of the co-intel problem of Dr. Martin Luther King; wrongheadedness, as far as I'm concerned, as it relates to the utilization of protecting this country.

A civil rights leader who happened to be outspoken against the heinous governmental acts of segregation and all of a sudden he became a major target of the Federal Bureau of Investigation, with any number of officers -- agents, if you will -- probing and looking over paperwork that he might have generated.

That smacks, as far as I'm concerned, of where we are today even though, Mr. Inspector General, you've indicated that it has been without malice, without intentions.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

And we all know that there is a phrase that says: A journey to a certain place is paved on that road with good intentions.

So I'm not very happy as to where we are today because I argued vigorously about the extensive powers that we were giving to the president of the United States out of fear.

And one thing that the Constitution reminds us, and certainly in the founding fathers, who left a tyrannical society to be free, that tyranny can get the best of us. And lack of control can get the best of us.

So I ask to the general counsel of the FBI: Did you determine what percentages of those letters that were sent without national security letters generated into terrorists responses or terrorist incidences or terrorist prosecutions? I'd be interested in that number.

And why don't you just answer that, yes or no, you have the percentage?

CAPRONI: I do not.

JACKSON-LEE: OK. I'd like to get the percentage, frankly.

CAPRONI: The directorate ordered a special investigation of the whole exigent letter instance, and we will brief this committee when we have the results of that.

JACKSON-LEE: And I will join my colleague on the other side of the aisle.

How quickly can you get that information?

This is about protecting the Constitution and securing the homeland, two very important jurisdictional responsibilities. And I happen to serve on both committees, Homeland Security and this.

So my question is, how soon can you get those numbers? It makes a real difference to know whether you generated potential terrorist threats that would secure the homeland or whether or not the FBI was on a fishing expedition.

CAPRONI: Congresswoman, let me assure you that that group was not on a fishing expedition.

But having said that, I understand that my assurance to this committee at this point isn't worth a lot. The Inspection Division is conducting the inquiry. They know that they have to proceed quickly. But I regret I can't tell you when they're going to be done.

But I will make sure that the director understands that you want it done as quickly as possible.

JACKSON-LEE: And certainly we wish the director well. We would have wanted to have his appearance before this committee, but we do wish him a speedy recovery.

CAPRONI: Thank you. I'll let him know that.

JACKSON-LEE: Mr. Inspector General, I assume you will say to me that you don't speculate, but let me quickly ask you a question.

And will you be thinking, the general counsel, on this question?

The president signed on the Patriot Act a signing statement, which indicated that he was going to interpret or have the act interpreted in a manner consistent with the president's constitutional authority to supervise the unitary executive branch and to withhold information.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

Just be thinking about that. And I want to know, did that give you a free ride? That's why I have legislation that indicates that agencies should not be running, I must say, amuck because of the signing statements.

Mr. Inspector General, what you looked at. And you've said it has not been intentional. Help me out, however. Don't you believe there should be restraints put in place, strictures put in place? And might the Patriot Act be entirely too broad to even be a valuable tool that would restrain people in balancing both security and, as well, balancing civil liberties?

FINE: I do believe that there needs to be controls. I do believe that there needs to be a balance, a balance of effective tools to prevent terrorism; at the same time, effective controls on the use of those tools.

And what was most troubling to us was that those controls were not implemented and not followed. And I share the concerns expressed by the members of this committee, and that's why we did the report.

FINE: We were not -- we were not restricted or limited in what we did.

And I know there was a presidential signing statement, but the department did cooperate with us. We did provide all the information that we had. We provided it in the most unclassified way we could, and the department actually did unclassify a fair amount of this information so that it could be fully aired.

And we also provided a classified report to this committee and other committees describing the additional information.

So we did what we could to identify the problems in this program.

CONYERS: The gentleman from Florida...

JACKSON-LEE: Mr. Chairman, could I just let the -- can she answer yes or no on the signing statement? Would you indulge me?

CAPRONI: The signing statement had absolutely no impact on how we interpret our national security letter authority.

JACKSON-LEE: I thank you.

CONYERS: The gentleman from Florida, Mr. Ric Keller?

KELLER: Thank you, Mr. Chairman.

Ms. Caproni, let me begin with you.

If the FBI didn't have national security letters as an investigative tool, you could get the same information via prosecutor through a grand jury subpoena or by going before a FISA Court and getting a court order, isn't that correct?

CAPRONI: Yes.

KELLER: And the concern that you have with those two options is that you essentially don't have the manpower -- I think you said it would, sort of, sink the system.

CAPRONI: I was responding to a suggestion that all of these should be obtained via court order. If that were the law, that would create substantial obstacles to our national security program.

KELLER: But that's why you aren't using in all cases the grand jury subpoenas or the FISA Court orders, because you don't have the manpower to do that and still do your investigations.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

CAPRONI: I would say it's perhaps slightly more nuanced than that. On grand jury subpoenas, there are cases where we don't have a criminal case open, so a grand jury subpoena is not an option.

Further, the whole philosophy of making sure that you're thinking -- we're thinking from an intelligence perspective rather than immediately cutting to the chase of a criminal investigation encourages agents to use national security tools versus criminal tools. The grand jury subpoena is a criminal tool.

KELLER: All right, let me follow up, because the challenge we have is getting this in the strike zone. We want you to have this information that you need as an investigative tool, but we want there to be some sort of check on your authority. And if you use the grand jury subpoena, for example, to get my phone records, I have the ability to move to quash that subpoena and have a judge hear it, correct?

CAPRONI: You only have the ability to do so if someone tells you that the subpoena has been served, which is not the typical route of a grand jury subpoena.

KELLER: OK, or if you went before a FISA Court, you have a set of eyes through the FISA Court judge looking at it, correct?

CAPRONI: That's correct.

KELLER: In terms of using the national security letter, let's say you served it on my phone company, the phone company's not necessarily looking out for my personal privacy interests, and so there's not a set of eyes looking at it, at least from an individual's perspective, right?

CAPRONI: And, again, that's the same as with a grand jury subpoena, that's correct.

KELLER: So all we have really is our inspector general as a check on the controls to make sure that you're applying it in an appropriate way.

CAPRONI: Well, again, I think this report has told us we internally have to do a far better job at making sure that we are maintaining internal controls over the use of this tool.

CAPRONI: I fully expect Mr. Fine to come back to visit us in future years, and will dutifully take us to task if we have not accomplished that.

KELLER: All right.

And, Mr. Fine, imagine a housewife in Orlando, Florida. And she does absolutely nothing relevant to terrorism or espionage. She's never met or spoken with a terrorist or a spy.

Based on your investigation, does she have any reason to worry about national security letters violating her privacy, by looking at her phone records, bank records or Internet search records?

FINE: I think that there are times when the FBI looks for telephone records of potential terrorists and looks to see who they've contacted or they've been in contact.

Now, it could be intentional contact; it could be inadvertent contact. And as a result of that contact, there can be efforts to look and see what telephone numbers have been called.

Now, if they have had no contact whatsoever with the subject of a potential terrorist investigation, it's less likely that there will be -- the records would be obtained here.

KELLER: Well, in framing my question, I said no contact, either writing or spoken.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

So let me ask you, based on your investigation, were there any situations where you saw national security letters being used when there was no relevance whatsoever to international terrorism or espionage?

FINE: We couldn't, in our review, look at all the investigative case files and say, "This was -- there was an adequate predicate; there wasn't an adequate predicate."

We looked at how they were used and whether on their face they were improper. So it's impossible for us to say that the relevancy standard was met.

One thing that we did find, however -- and I would note this -- is that, in many cases, the counsel of the FBI field offices, either the chief division counselor or the assistant counsel, did not aggressively and independently look for that. And they're the ones who should be checking on that. They're the ones who need to be sure that there's adequate predicate for this investigation.

And we saw, in many cases, that didn't happen, that they acceded to the wishes of the -- or the arguments of the case agents or the special agents in charge, without independently and aggressively looking at that...

KELLER: Let me cut you off there because I have one final question.

Ms. Fine (sic), can you give us an example to help make your case, if you have one, as to what's a scenario where a national security letter is your best investigative tool because, for whatever reason, a grand jury subpoena or a FISA Court order is insufficient?

CAPRONI: Any time I would say that we were at the very beginning of an investigation -- say, for example, after the London bombings, when the British authorities provided us with telephone numbers of the British bombers, so we were looking to see did we have anyone in the United States that had telephone contact with the London bombers -- in my view, the appropriate way to pursue that investigation is via national security letter.

KELLER: Because you wouldn't have time under the other options?

CAPRONI: Well, we wanted to know that very quickly. And, again, I think the American people would want us to know very quickly after the London bombings took place whether we had any cells or groups of people who were tightly related to the London bombers.

So we needed to move very quickly. And, in fact, the investigators did move very quickly on that to figure out who here was connected to there and was it an innocuous connection or was it a dangerous connection.

KELLER: Thank you.

My time has expired.

CONYERS: The distinguished gentlelady from Los Angeles, California, Maxine Waters?

WATERS: Thank you very much, Mr. Chairman. May I ask: Were these witnesses sworn in?

CONYERS: They were not.

WATERS: May I respectfully request that they be sworn in?

CONYERS: Too late.

WATERS: Then, Mr. Chairman, I suppose we're going to have to rely upon them, particularly the general counsel, continuing to tell us that they're acting within the law.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

I shall proceed with my questions.

CONYERS: If the gentlelady will yield...

WATERS: Yes.

CONYERS: ... testimony before this committee can constitute a violation in and of itself.

(CROSSTALK)

CONYERS: A misstatement -- any deliberate misstatements.

WATERS: Well, I would have preferred that they be under oath. But, however, the chair has made that decision and I shall proceed.

Let me just ask about the use of these exigent letters. As I understand it, these letters are used basically to get around having to get the NSL letters, is that right, Mr. Fine?

FINE: These letters were used in advance of or in lieu of national security letters, that's right.

WATERS: And there was information collected as a result of these letters, particularly the operation, I believe, that was set up with the contract with the three telephone companies or telecommunications companies, is that correct?

FINE: Well, there were contracts with the telephone companies so that they would provide information to the FBI on an expedited basis.

WATERS: Ms. Caproni, do you still have contracts with those telephone companies, any other telephone companies, or any other private businesses to supply you information in the manner that those companies did?

CAPRONI: We continue to have contracts with the telephone carriers that obligate us to provide them with appropriate process to get records.

I don't -- I can't answer the balance of your question. I don't know if we have other contracts with other private parties.

The telephone companies, it made sense because of the volume of our requests.

WATERS: How much do you pay them for the service? How much are the taxpayers paying the telephone companies that they pay to provide them services to spy on us?

CAPRONI: I don't know what the dollar value of the contracts are.

WATERS: You have no idea?

CAPRONI: I actually don't.

WATERS: You've never heard any discussion about it?

CAPRONI: I'm sorry, I don't. I just don't know what the amount is.

WATERS: Information was collected on millions of Americans using this as a tool. Now that you know that they were innocent, they probably should not have been under investigation, has all of this information been purged and gotten rid of?

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

CAPRONI: We did not collect records on millions of Americans through...

WATERS: How did it work?

CAPRONI: The exigent letters were provided to the carriers, which promised future process. That future process, unfortunately, it was not always promptly provided.

WATERS: What did they do? What did they do?

CAPRONI: What did who do?

WATERS: The companies. How did they mine the information? And did they mine information of innocent people?

CAPRONI: The carrier has provided us with toll billing information, which was then placed into our databases. There is no connection between their databases and our databases. The information comes out electronically and moves into ours.

But, again, we're talking about -- I believe that the number of numbers at issue, according to the inspector general, is somewhere in the neighborhood of 3,000.

And it is my belief, though, again, we'll have to wait and see what the special inspection finds, that all of those numbers were tied to authorized investigations.

To the extent any were not, the records will be removed from our databases and destroyed.

WATERS: When will they be removed? How long will it take?

CAPRONI: Again, I am anticipating that that special inspection will take a couple of weeks, at least, but probably -- I just actually don't want to speculate.

As I have...

WATERS: Did you have a court order relative to your contracts with these telephone companies?

CAPRONI: No, ma'am.

WATERS: Was there a court decision relative to the manner in which information was obtained?

CAPRONI: The information was obtained from the carriers pursuant to -- it was supposed to be obtained pursuant to the laws of ECPA.

WATERS: But they were not.

CAPRONI: Well, again, as Mr. Fine has indicated, there were these exigent letters that were used.

What we're trying very hard to do is to unravel and to make sure that we do not have the records of anyone who -- as to which there was not -- it wasn't relevant to an authorized investigation.

(CROSSTALK)

WATERS: How long have you been trying to do this?

CAPRONI: We began the process with them last fall. And we are -- we, within OGC, are to the point that if they

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

cannot demonstrate to our satisfaction very quickly, then any of those records have to be removed from the database and destroyed.

WATERS: Certificate letters: Are you still issuing certificate letters?

CAPRONI: No.

WATERS: When did you stop?

CAPRONI: Shortly after OGC learned about them, that process was stopped.

We entered into discussions with the Fed, the Federal Reserve Bank, in terms of whether or not it required a national security letter. There was some back and forth between lawyers that the decision was made that they would prefer a national security letter, and we've always now provided them.

WATERS: So you collected information using these certificate letters. Had that information been destroyed?

CAPRONI: No.

WATERS: When are you going to do it?

CAPRONI: I don't believe we're going to do it.

WATERS: Why are you going to keep information that was improperly collected on financial records of innocent people? Why would you keep it?

CAPRONI: One, it's not innocent people. And, second, it wasn't improperly collected.

The Federal Reserve Bank is not directly covered by the right to financial privacy. They can ask for a national security letter, which they now have done. And because they're asking...

WATERS: Well, why did you stop using certificate letters if they were legal and proper?

CAPRONI: Because we thought the better process was a national security letter. And the Fed asked us to provide them with national security letters.

WATERS: How have you determined whether or not the information that you collected was on individuals who were suspicious, guilty, had committed a crime? I mean, how do you determine whether or not these people are innocent and the information should be destroyed?

CONYERS: The gentlelady's time has expired.

Please answer the question.

CAPRONI: Certainly.

The issue is whether the information is relevant to an investigation. There are times when we gather information that is relevant to an investigation but it turns out that the person was not engaged, for example, in terrorist financing.

Now, we don't then destroy the information, though the investigation is closed. So it's much like any other information that's gathered during the course of an investigation.

And the issue of whether that policy will continue is a matter that's under discussion by a group that's being chaired by the DNI, in terms of whether we should or we should not continue to retain information that's gathered via national

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

security letters after the investigation is closed.

CONYERS: The gentleman from Virginia, Mr. J. Randy Forbes?

FORBES: Thank you, Mr. Chairman.

Mr. Chairman, I hope I can emulate your very calm and fair manner of handling this committee.

And I just want to tell the witnesses what I said at the beginning. I want to thank you both for being here. We know you have a tough job, and we appreciate you coming in here and answering our questions today.

I've listened to the committee as we've gone through this process, and we've had testimony from The Washington Post, we've had testimony from members of the audience, testimony from members of this committee. You're the only witnesses we have here.

And I think that you get the message, both of you, you had it when you came in here, that no one on this committee condones any of these lapses or feels that it's not urgent that they be corrected and corrected as quickly as possible.

We're also grateful that this committee requested this audit, because, Mr. Fine, through your good work we were able to find out what these problems were so that we can correct them.

The other thing, Ms. Caproni, you've been asked to take a lot of messages back to the FBI, all of which are good and valid messages.

But another one I want to ask you to take back today is that, although the FBI messed up in handling the NSLs, I wanted you to take a message back to those agents in the field who I know are working around the clock, they're away from their families a lot of times, and thank them for not messing up on what Mr. Fine said was one of their key missions. and that was to detect and deter terrorism and espionage in this country.

Because if you had messed up on that one, we'd have a lot more people in this room and we'd be a much harsher hearing than what we're having today.

The other question I'd just like to ask either of you to respond to, do either of you have any evidence today that anyone in a supervisory position gave instructions, either expressly or impliedly, to any person under his or her supervision to misuse the NSLs?

CAPRONI: Not to my knowledge.

FORBES: Mr. Fine?

FINE: We didn't find that evidence. We did not find that there was an intent by people who knew they were misusing it to misuse it. So, no.

On the other hand, we did not do a thorough review of what people up and down the line knew and did. So we reported what we found.

FORBES: And that's being conducted, as I understand it, now. Is that correct, Ms. Caproni?

CAPRONI: Correct.

FORBES: And if you find that information, you'll present that back to the committee, correct?

CAPRONI: Absolutely.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

FORBES: Second question for either of you: Is there any evidence that any member of the FBI or the Justice Department provided any information, either orally or in writing, to this committee or to Congress which they knew to be inaccurate or false?

CAPRONI: Not to my knowledge.

FORBES: Mr. Fine, you don't have that?

FINE: I don't have that information, no.

FORBES: And just the balance that we've talked about -- we know the harm that comes from violation of privacy interests of our citizens. That's huge.

But I wish you would go back, Ms. Caproni, and, again, just take a minute and talk about what Mr. Fine has put in here about -- it says that these tools are indispensable to the FBI's mission to detect and deter terrorism and espionage.

We know there's been a lot on your plate since 9/11 and you had to do that. Can you tell us with as much specificity as you can exactly how these NSL letters have helped to do and accomplish that mission?

CAPRONI: Again, national security letters provide the basic building blocks of an investigation, and starting with phone records. Phone records are critical to the counterterrorism agents to figuring out who is connected to whom. And that permits us to trace foreign terror acts that have occurred, obviously, since 9/11 and trace them in to individuals who are in the United States, and to determine whether those individuals are up to no good or, in fact, there's just an innocent connection.

But for national security letters, I don't know how we would do that.

They've also been absolutely indispensable in the area of terrorist financing. We've done a tremendous amount of work of getting bank records on individuals that we believe were funneling money to foreign terrorist organizations overseas.

And again, without national security letters, I'm not -- you know, could we go through a FISA order? We probably could. But we certainly couldn't do that very efficiently.

So a national security letter is an efficient way for us to get the basic building blocks of an investigation.

FORBES: Have they stopped any terrorist attacks that you know of that could have possibly happened in the United States? You may not have that information.

CAPRONI: I'm sorry, I don't.

FORBES: OK. That's good. Thank you both.

And, Mr. Chairman, I yield back the balance of my time.

CONYERS: I thank the gentleman.

The chair recognizes Stefan Cohen, the gentleman from Memphis, Tennessee.

COHEN: Thank you, Mr. Chairman.

Stephen, yes, that's all right.

(LAUGHTER)

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

But you can call me "Stefan."

(LAUGHTER)

CONYERS: Stephen.

COHEN: Thank you, sir.

Mr. Fine, did you do any study of the people whose records were looked at illegally for any similarity in demographics?

FINE: No. We looked at whether they were U.S. persons or non- U.S. persons. But, within those categories, we did not look at the demographics of those individuals.

COHEN: Ms. Caproni said they were all within investigations that were ongoing. Did you find that to be true also?

FINE: We could not verify that they were all connected to an ongoing investigation.

I know the FBI is trying to do that now. But as part of our audit, we could not do all of that.

COHEN: Do you think it might be a good idea to look at those people, so see if there are any demographic consistencies, if there's a group of the American public that might be looked at in a closer manner than others and that that might...

FINE: It's possible. That would be quite an undertaking. And one also has to realize a lot of these are not on individuals. They're on telephone numbers and things like that. There are certainly consumer credit reports and other things that do relate to individuals.

So that kind of a review is possible, but it would be incredibly intensive and require additional resources while we're trying to comply with this committee's and the Congress' directive to do a review of the use of them in 2006 according to the guidelines that were set out here.

COHEN: Thank you.

Ms. Caproni, you said that these were all tied to investigations, is that correct?

CAPRONI: I said that I believed they were all tied to investigation, and that's what we're trying to work through with that unit now.

COHEN: If you find that they're not tied to investigations, could you make a report to this committee of who those individuals were and why their records were sought when they weren't tied to investigations?

CAPRONI: Yes. We will provide this committee with what we find through the course of the special inspection.

If I could just say, though, based on -- so there's no misunderstanding -- the unit at issue typically gets simply a telephone number. So they don't know -- that's part of what they're charged with finding out is who belongs to this telephone number? What are the toll billing records for this phone number? So the name of the person associated with the phone number is typically not part of what CAU does.

And for the exigent letters, to my knowledge -- though, again, the special inspection will reveal much more in terms of the ins and outs of what they were doing -- they were working off of telephone numbers and not off of names.

COHEN: In the report, it says that some of these violations demonstrated FBI's agents' confusion and unfamiliarity with the constraints on national security letter authorities. Other violations demonstrated inadequate supervision over

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

the use of these authorities. This is from Mr. Fine's statement.

Ms. Caproni, do you think that this is, maybe, indices of a systemic problem in the FBI, where the agents have confusion and unfamiliarity with other policies and other laws. And if so, are you doing something about it?

CAPRONI: Congressman, that is exactly what I'm concerned about. And in the discussions that we've had -- and I can tell you that we've had a lot of soul searching at the FBI since then -- this is, you know, we got an F report card when we're just not used to that. So we've had a lot of discussions about this.

And one concern is, are we -- you know, most of the agents grew up, the agents my age in the FBI, all grew up as criminal agents in a system which is transparent, which, if they mess up in the course of an investigation, they're going to be cross-examined, they're going to have a federal district judge yelling at them.

CAPRONI: The national security side occurs largely without that level of transparency.

And our concern is, and what this report has shown us, is that we have simply got to do a better job making sure that, although the actions that are taken in national security investigations are typically taken in secret and they don't have the transparency of the criminal justice system, that that imposes upon us a far higher obligation to make sure that we have a vigorous compliance system. that we have in place the training that is necessary. that we retrain agents. that when agents are working in this area...

COHEN: I appreciate that. I think you're getting...

CAPRONI: ... we make sure they know.

COHEN: I think that's what we need. And I appreciate your candor.

There's some signage in the Capitol, and one of them's a statement by Brandeis -- Louis Brandeis, and something to the effect that the greatest threats to liberty come from insidious men of zeal, well-meaning but without knowledge or understanding.

And I think that you'll find that if our agents, FBI agents, even though well-meaning and zealous, don't know what they're doing, then it's a threat to people having faith in the whole system.

And I hope you'll correct that. And I feel confident you will.

CAPRONI: You're absolutely correct. And we will.

COHEN: Thank you.

CONYERS: I thank the gentleman, Stephen Cohen.

(LAUGHTER)

And the chair recognizes now the gentleman from Virginia, Bob Goodlatte.

GOODLATTE: Thank you, Mr. Chairman. And thank you for holding this hearing.

And, Ms. Caproni and Mr. Fine, thank you for your testimony today. These are very serious concerns. And we appreciate your helping us understand how they occurred, why they occurred, and what is being done to correct them.

I have several questions I'd like to ask, starting with you, Ms. Caproni.

In Mr. Fine's report, on page eight, paragraph three, he notes: "In addition, we found that the FBI had no policy

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

requiring the retention of signed copies of national security letters. As a result they were unable to conduct a comprehensive audit."

Can you explain why something as important and serious as a national security letter would not have a signed copy retained in the records of the bureau?

CAPRONI: I can say that there were different processes in different field offices but, no, I can't. I mean, there's no reason why there wasn't a policy that said, "You have to keep a copy of the signed copy."

What we keep, which is typical of how our records are, is the carbon copy, in essence, which is typically initialed.

But no, in the world of Xerox machines, there's no reason why we hadn't told people to hang onto a signed copy.

GOODLATTE: Mr. Fine, did you draw any further conclusions from that? And do you know why they were not retained? Or is there any...

FINE: They weren't retained because there wasn't a clear policy that was enforced.

GOODLATTE: No ulterior motive that you know of?

FINE: We don't believe there is an ulterior motive. But this was an example of the incredibly sloppy practice that was unacceptable.

GOODLATTE: I agree.

Let me ask you: When did you first learn of the problem with the FBI's improper use of exigent letters?

FINE: Well, we began our audit in, as required by the Patriot reauthorization act, around the beginning of 2006. As you can see from this report, there are a lot of issues. And we did interviews and document request and field files.

FINE: I think, sort of, the first indications that we learned about it were in the spring or summer of last year, but we had to work through those issues.

GOODLATTE: And who did you learn that from?

FINE: We learned it from, I believe, people in the Office of General Counsel, the National Security Law Branch of the FBI, about these issues. I think that's the first people we learned it from -- as well as review of documents and e-mails and things like that.

GOODLATTE: And what steps have you taken to ensure that the practice was stopped?

FINE: And what steps have we taken? The steps we've taken is to inform the FBI about the unacceptability of this practice, to note it, to report it, to let the people who were in charge of the FBI and the general counsel's office know about it, and make a recommendation that it do stop -- that it does stop.

GOODLATTE: When did you make that recommendation?

FINE: I think we made the recommendation when our report was issued to the FBI in draft, and I think that was in either December or January of this year -- December of last year or January of this year.

GOODLATTE: And, Ms. Caproni, has that practice been stopped?

CAPRONI: Yes.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

GOODLATTE: And what steps have you taken to ensure that it does not persist in any of the offices of the FBI?

CAPRONI: Well, first, we're trying to find out whether it did happen in any office other than the unit at headquarters. And we should know that answer probably by the end of this week or sometime next week.

Second thing is, the practice of providing a letter with a promise of future legal process has been banned. And, again, we are also developing a vigorous compliance program to make sure that we don't simply make the rule, but we actually have in place some kind of process to make sure that the rules are being followed.

GOODLATTE: Current law authorizes a full credit report request for only counterterrorism investigations. The inspector general discovered two instances in the same field office of a full credit report request under counterintelligence investigations.

How is this being corrected?

CAPRONI: This is being corrected by we -- the deputy director ordered a full audit of every counterintelligence file that has been opened since January 1, 2002. This authority went into effect in the Patriot Act. So realistically we think the earliest one could have been issued would have been 2002.

So they have to review every file since then in which a Fair Credit Reporting Act NSL was issued and find out if they have any full credit reports. If they do, they need to remove them from their files and report it as a potential IOB violation.

Those will, in turn, be reported on to the IOB.

GOODLATTE: One last question: In at least one instance, a national security letter issued under the Electronic Communications Privacy Act was determined by the inspector general to be seeking content. How was this remedied?

GOODLATTE: And what steps do you field agents take to delineate between content and transaction information?

CAPRONI: In that case, there was no need to remedy it because the Internet service provider refused to provide us with any records. So we actually did not have an overcollection.

GOODLATTE: And have you remedied the...

CAPRONI: Yes.

GOODLATTE: ... request? I mean, they shouldn't be asking for that. This was a big issue when we wrote the Patriot Act...

CAPRONI: Correct.

GOODLATTE: .. and was subject of a great deal of discussion with the administration about making sure that we had a clear line between what could be requested and what could not be requested.

CAPRONI: The statute defining electronic communication transactions records actually doesn't define the term. And there had traditionally been the debate that says, "So we'll leave it up to the ISP to decide what is content and what is not."

We think that's a trap for the unwary, it's bad for our agents, and that we do better with bright lines.

And so OGC -- we're in the process of making sure that we have a list that makes sense; what is content and what isn't.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

In the abstract, that seems like a very clear line. In practice, it is not. There are some difficult issues because some of the answers revolve around how the ISP keeps their records.

So we're working on it. My anticipation is that within the next week or two we will have out to the field, "These records you can seek; these records you cannot seek," and it will be a very bright line.

GOODLATTE: Thank you, Mr. Chairman.

CONYERS: The gentleman from Georgia, Mr. Hank Johnson?

JOHNSON: Thank you, Mr. Chairman.

In these reports that I have read, it indicates that there were three phone companies that the FBI, particularly the FBI Communications Analysis Unit, the CAU, contracted with three telephone companies between May 2003 and March of 2004.

JOHNSON: Who were those telephone companies?

CAPRONI: The telephone companies were AT&T, Verizon and MCI, which has now been acquired by Verizon.

JOHNSON: Now, are those contracts still in force at this time?

CAPRONI: Yes, they are.

JOHNSON: And are there any other phone companies that are contracted with the FBI through the Communications Analysis Unit or any other unit of the FBI?

CAPRONI: Not through the Communications Analysis Unit. Broader than that, I don't know. We may have contracts -- not for this sort of information. We may have other contracts with phone companies, but not like this.

JOHNSON: And nobody put a gun to these telephone companies' heads and made them sign the contracts, did they?

CAPRONI: No.

JOHNSON: They were just simply agreements with the FBI and the phone company.

CAPRONI: Correct.

From our perspective, because these originated, given the volume of our requests, that this permitted us to get our records very quickly.

JOHNSON: Well, I understand.

And then the phone companies received compensation for engaging in this contract with the FBI, is that correct?

CAPRONI: That's correct.

JOHNSON: And these -- this compensation, was it merely for expenses or was there profit involved, or you have no way of knowing?

CAPRONI: I don't know.

JOHNSON: And, really, you don't really care, as long as you get the information, correct?

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

CAPRONI: Again, from our perspective, the goal was to get the information in a form that is readily usable for us, so that we don't have -- some phone companies give us paper records. That requires a lot of data entry.

JOHNSON: All right. I understand.

And earlier in your testimony, ma'am, you stated that the phone companies were responsible for a lot of the errors that are cited in the compliance with the national security letters.

CAPRONI: We do see third-party errors, correct.

JOHNSON: You saw a substantial number. And so you are placing upon the phone company the obligation to properly document whether or not there has been a follow-up with an exigent letter.

CAPRONI: Oh, no, sir. There are two separate things.

I do not excuse our lack of recordkeeping in connection with the exigent letters. They did keep the records, which was fortunate.

JOHNSON: And it's important to note, Mr. Fine, that your analysis of the FBI's compliance with the Patriot Act found that there were woefully inadequate mechanisms for the collection of data on these national security letters.

JOHNSON: In other words, the recordkeeping by the FBI was woefully inadequate as far as the issuance and follow-up on these national security letters and also the exigent letters, isn't that correct?

FINE: We did find serious and widespread misuse and inadequate recordkeeping, absolutely.

JOHNSON: And do you have any idea, Mr. Fine, how much the telecommunications companies were paid for their so-called contract with the government?

FINE: I don't know it, no.

JOHNSON: All right.

Which agency -- can you, Ms. Caproni, provide my office with that information, along with copies of the contracts between the CAU and the phone companies?

CAPRONI: I have great confidence that we're going to get a number of questions for the record after this, and I'm assuming that will be one of them and we will respond appropriately.

JOHNSON: Will it take a subpoena for us to get that information?

CAPRONI: I don't believe so. I don't know what's in the context...

JOHNSON: Will you provide it...

CAPRONI: I don't know if there are any sensitive issues...

JOHNSON: Will you provide it to my office?

CAPRONI: Again, we'll respond to questions for the record as they come in.

JOHNSON: All right.

Why is it that, if the NSLs are the FBI's bread-and-butter investigative technique, could the inspector general only

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

identify one terrorism prosecution out of 143,074 people whose letters were -- or who investigatory information was obtained on?

CAPRONI: Again, Mr. Fine can explain his methodology.

But I think the issue, and the difficulty of that question is that because there was no congressional -- we were not legally obligated to tag the data, so tracing it through is difficult.

JOHNSON: So one out of 143,000 -- how does that equate into being the bread-and-butter investigative technique for uncovering terrorism by the FBI?

CAPRONI: Again, we disagree that in only one case did NSL data contribute to a criminal prosecution.

JOHNSON: But would you say more than 10 or less than 10?

CAPRONI: I don't know. It is my belief that virtually every...

JOHNSON: But you don't know?

CAPRONI: ... counterterrorism case that began in its normal course of affairs is likely to have a national security letter used sometime during it.

JOHNSON: And it's also...

CONYERS: Time has expired.

JOHNSON: Thank you.

CONYERS: And, Mr. Johnson, any records that you request will come to the committee and then you will be advised.

The chair is pleased now to recognize the gentleman from Florida, Mr. Tom Feeney.

FEENEY: Thank you very much, Mr. Chairman.

And, earlier, Mr. Smith alluded to your illustrious basketball career. I wish. I went to the same high school as Mr. Fine. He graduated a few years before me. And I wish I'd have had a jumpshot like Mr. Fine did, but not nearly so much as I wish I would have been able to hit a fastball like Mr. Reggie Jackson, who graduated a few years before Mr. Fine did.

But we thank you for your work.

By the way, none of us is the most famous graduate, because Benjamin Netanyahu, former prime minister of Israel, is a Cheltenham High grad.

I had to get that plug in.

We are very grateful for your work here, because a lot of us were supporters of the Patriot Act, but only with some serious restrictions. And I guess the first question I want to ask you, to remind people, is that it was the reauthorization of the Patriot Act that actually required the report that you've just completed, is that right?

FINE: Yes.

FEENEY: And I hope that not just your report, but the tenor of the questions from supporters of the Patriot Act as

well as the critics is being listened to very carefully in the Justice Department and the FBI.

FEENEY: We have got to get this balance correct.

And nothing could be more critical, because some of the most unthoughtful critics of the Patriot Act candidly will be the first ones when there's another 9/11 and when we didn't get the information accurately ahead of time to stop, maybe not 3,000 or 4,000 people, but 300,000 or 400,000 people -- they'll be the first ones jumping on the administration, the Justice Department and the FBI for not doing its job.

But those of us trying to strike a thoughtful balance between civil liberties and between the need to protect America from this new threat are very, very concerned about what we've heard.

And if the FBI doesn't take this to heart, we will correct the problem. I don't think anybody could have said it better than Jim Sensenbrenner -- again, a supporter of the Patriot Act -- who said that the overreaching that's apparent here within the FBI is going to erode support, if it hasn't already, from very important national security initiatives.

And I would hope that everybody down at Justice is listening, because this is the supporters -- people like Lungren and Feeney and Sensenbrenner -- that are telling you this isn't right, and it can't continue.

Mr. Fine, do you have an opinion as to whether or not the serious problems that you've discovered in initial compliance with the Patriot Act are largely because of ambiguities or poorly structured legislation? Is it statutory language that was the problem largely here, or is it abuses within the FBI in compliance?

FINE: I don't think it was the statutory language that was ambiguous. I think it was the execution of the policy by the FBI that was woefully inadequate.

FEENEY: And just to follow up, can you identify or does your -- does your report and investigation lead you to conclude that there are any important statutory improvements we could make?

I realize it's not in your typical arena to give us advice, but are there any specific pieces of advice that you would give the Congress in terms of oversight or statutory reforms here?

FINE: Well, you're correct: It is not in my arena to do that. What I try and do is present the facts to this committee and Congress, and let the facts lead this committee and Congress to do what they believe is appropriate.

There is one section of the report that does talk about an ambiguity in the meaning of toll billing records. I think there ought to be something done about that, because that was a concern of what that meant, and it should be clarified.

I do think in...

FEENEY: Could the A.G. do that by opinion?

FINE: I don't think so. It has to be done by Congress.

I do think that the committee does need to strike a balance and, sort of, balance the need for protections and controls over civil liberties with the need for tools to prevent and detect and deter terrorism.

And that's the difficulty in this task. And that's the real concern that we have about how the FBI implemented this.

FEENEY: You said you sampled 77 case files, your report indicates. How many case files are there all together, roughly?

FINE: That I couldn't tell you.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

FEENEY: Do you believe that the 8,850 failed reportings are systemic and that if you extrapolate we'd probably see that elsewhere?

FINE: I do believe that the files we looked at were a fair sample and that there's no reason to believe that it was skewed or disproportionate. We didn't cherrypick them.

FEENEY: Do you have any reason to believe that there were more abuses in the 8,850 requests that were not properly reported? Are they any more likely to be abuses of civil liberties or the law or the A.G.'s rules than the requests that were properly recorded?

FINE: Well, we don't know how many requests were not recorded in the FBI's databases. There were some problems with the database structurally so that things weren't in there. There were delays in entering the database so Congress didn't get the information they wanted.

And when we looked at the files, there were NSLs that were in the files that didn't go into the databases -- approximately, I think it was, 17 percent of the ones we found weren't in the database. Now, that's a significant number.

And now I know the FBI's trying to find them in the database as we speak, but we have no confidence in the accuracy of that database.

FEENEY: Finally, if I could, Mr. Chairman, Ms. Caproni, you alluded to the culture of the FBI, which was traditionally a crimefighting institution.

Some people have called for an MI5 type of intelligence agency with a different culture. And it might be interesting that you take back the interest that some of us in Congress have. If the FBI can't change its culture or have a separate culture for intelligence than it has had traditionally, we may very much need a different type of institution to get intelligence right to protect this country on a day-to-day basis.

CAPRONI: Again, I believe that we can do this, we're going to do this, we can get this right, and we're going to get it right.

FEENEY: Mr. Chairman, I yield back the balance of my time.

CONYERS: Thank you. There wasn't any left.

(LAUGHTER)

FEENEY: That's why I did it.

(LAUGHTER)

CONYERS: I see.

OK. We're now going to recognize the gentleman from California, Mr. Adam Schiff.

SCHIFF: Thank you, Mr. Chairman.

Inspector General Fine, you've said that you didn't find that any of the violations were deliberate or intentional.

SCHIFF: And yet you also report the issuance of blanket NSLs, which, to me, appear to be an effort to cover up what was recognized to be flawed issuance of these exigent letters.

Given that NSL letters are supposed to be case-specific, the NSLs were a blanket violation of the law, weren't they? And how can they be described as unintentional or anything but deliberate?

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

FINE: I think what you're referring to, Congressman Schiff, is issuance, of what we've heard about, of blanket NSLs in 2006. We haven't reviewed 2006 yet. We reviewed 2003 to 2005.

We've heard about this. It happened past the review period. And we're concerned about it, and we'll look at that.

SCHIFF: Well, Ms. Caproni, in your briefing on the Hill last week, you acknowledged that when agents realized that they had been issuing these letters -- these exigent letters saying that subpoenas were forthcoming when they were never forthcoming, that blanket NSLs were issued as a way of basically trying to clear up or cover up or in other words make up for the failure to use correct processes in the past.

Assuming those are the facts, Inspector, doesn't that show a level of deliberateness and intention that far exceeds what you describe in your report?

FINE: It certainly shows us concern, and what were they thinking? They clearly were not following the procedures. They clearly were not providing NSLs in advance or even quite reasonably soon thereafter. And it did give us concern.

And there were a lot of people who did this. It was done as a sort of a routine practice, which is in our view completely unacceptable.

But I am -- I think it is important for the FBI to look at this and to interview these people and find out what happened, up and down the line, and we will be looking at it as well in 2006.

SCHIFF: Well, even the false statements themselves, these exigent letters that said that subpoenas were forthcoming when they weren't -- let me ask you, Ms. Caproni, if a local cop in the city of Burbank, in my district, wrote letters to the phone company or went out and served letters on the phone company saying that federal grand jury subpoenas would be forthcoming, because that local cop wanted to get information, that maybe they couldn't get another way or couldn't get as quickly another way, and you learned about this practice, that cop would be under federal investigation, wouldn't they?

CAPRONI: Congressman, I really don't know. I don't think you've given me enough facts to say that whether that would or wouldn't be (inaudible).

SCHIFF: Well, a local police officer, acting under color of federal law, demanding records that -- claiming a federal process that's nonexistent, that wouldn't be an issue for federal investigation?

CAPRONI: It would certainly be troubling, much as the practices that were taking place in the CAU unit are troubling.

SCHIFF: Well, you know, having worked in the corruptions section in the U.S. attorney's in L.A., I can tell you, it would be more than troubling. You'd have FBI agents assigned to investigate that local cop.

It doesn't seem to me any different to have FBI agents giving telecommunications providers letters saying that subpoenas are forthcoming when they're not.

When did your office discover that these old New York form letters were being used to get information?

CAPRONI: Sometime in '06.

SCHIFF: You know, there's a report in The Washington Post indicates the head of the Communications Analysis Unit, the same unit that drafted most of these letters, warned superiors about the problems in early '05. Do you know anything about that?

CAPRONI: I know what I've read in the paper. And I know that the Inspection Division is going to do a full

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

inspection of this to see what exactly the unit chief said...

SCHIFF: Well, I'm asking you beyond what you've read in the paper, and we all know what the I.G.'s going to do.

When did you first learn about the fact that the head of the unit that was drafting these letters had warned superiors?

Do you know who those superiors are?

CAPRONI: I don't know who he says he warned.

SCHIFF: Were you warned by him?

CAPRONI: No.

SCHIFF: Do you know if anybody in your office was warned by him?

CAPRONI: I'm not sure that I even necessarily agree that there was a warning.

I don't -- I know that there were -- and I knew generally that there were some what I understood to be bureaucratic issues within that unit. That did not include...

SCHIFF: You keep on describing these bureaucratic issues. I mean, I find an interesting, kind of, mix of acceptance of responsibility in your statement and denial of responsibility. You seem to accept responsibility for mistakes others made, but acknowledge very little responsibility on behalf of the office you run.

It's primarily your office that is intended to advise the agents about how to comply with the law, particularly in an area where the courts aren't scrutinizing it, as you pointed out, in a process that lacks transparency.

SCHIFF: Isn't that fundamentally the job of your office?

CAPRONI: That is fundamentally the job of my office.

CONYERS: The time of the gentleman has expired.

The chair recognizes Louie Gohmert of Texas.

GOHMERT: Thank you, Mr. Chairman. I appreciate that.

And I am very pleased that, when we renewed the Patriot Act, we did insert the provision that would require this inspector general report so that we could find out this information that is so very important.

In your report, your indications, Mr. Fine, was the FBI did not provide adequate guidance, adequate controls, adequate training on the use of these sensitive authorities; oversight was inconsistent and insufficient.

And Ms. Caproni, as I understood Director Mueller to say last week that he took responsibility for the lack of training and experience. And that troubled me a great deal.

You'd indicated earlier that people of, I guess, our generation and especially those in the FBI have grown up with accountability, knowing that you're going to be cross-examined. And yet it seems that the overzealousness that Mr. Cohen spoke of often is found in maybe new agents that don't have the time on the ground, the experience.

Wouldn't you agree that's sometimes found in newer agents that lack the training and experience?

CAPRONI: I don't know in this case if this is an issue of young agents versus old agents. I just don't know the

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

answer to that.

GOHMERT: Well, are you familiar with the new personnel policy that this director instituted in the FBI that's affectionately -- or unaffectionately -- called the up-or-out policy?

CAPRONI: Yes, sir, I am.

GOHMERT: And, you know, I appreciate the director last week saying that, "We welcome more oversight." I appreciate your openness in that regard.

But just in my couple of years of being in Congress is it seemed to me that the FBI, at the very top at least, was not interested in oversight and was set on intimidating anybody that really wanted to pursue that.

I know we have one members of Congress, a former FBI agent, who had indicated to me that because many of us who are very familiar with many FBI agents, we've been hearing that this policy was causing the FBI to lose some of their best supervisors.

The policy basically, as I understand it: Once you've been a supervisor for five years, then you either have to move up to Washington or move out; that you can't be a supervisor; and that we've lost many of our best supervisors, which has put new, inexperienced people in supervisory capacities; and that this was something that Mike Rogers, a former FBI agent, a member of Congress, wanted to talk to someone about. And when he finally was able to get somebody to agree in a supervisory position, he goes back to his office, and his whole office staff is out in the hall because the FBI's come over and done a sweep of his office that was really unnecessary and seemed to be more about intimidation.

GOHMERT: One of the most outspoken critics of the FBI the last couple years has been Kirk Weldon, and we know that back in September and October, the FBI announces, "Well, gee, he's under investigation," just at a perfect time to get him defeated.

And so, it seems that -- and then we find out there were all these 143,000 letters that were inappropriately requested, well, gee, somebody asks tough questions of FBI personnel, they may very well be the 143,001st letter in the next batch inquiring about their own records; that there has not been this desire for oversight, but there's been quite some intimidation.

So I'm curious, has there been any revisiting of this up-or-out policy to get rid of the best-trained and experienced supervisors, since this lack of training and experience and inadequate guidance and controls has come to light?

CAPRONI: Congressman, the period of time covered by Mr. Fine was at a period of time when those supervisors would have still been in place.

What we've seen, actually, is that the five-year up-or-out has encouraged people to bid for and seek promotion to higher positions, which has been a net positive.

Now, I know that you have an interest in this, and I know that there were agents who were not happy about the policy. The director feels very strongly that it's an appropriate policy, that it does move good supervisors up in management so that they have a greater span of control, so that we can further benefit from the skill set that they have from their tenure at the bureau.

GOHMERT: So the answer is no, you're not revisiting the policy, is that your answer?

CAPRONI: That is correct.

GOHMERT: OK, just wanted to wade through and get to the answer.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

Thank you.

Now, with regard to these letters, it is deeply troubling, because we've been hearing about how important they were in order to get this information, but, you know, we had assurances from everybody, from the A.G. on down, that there was adequate oversight, that there was adequate training.

What suggestions -- since you're not changing any personnel policies, what actual, structural policies within the FBI are going to change to make sure that there would be adequate oversight, just in case the NSLs were allowed in the future?

CAPRONI: Again, we're going to do substantially more training. Agents are now being placed into career paths and they're going to be required, after their time at Quantico, to return to Quantico for, sort of, a post-graduate period. That will have extensive training for those agents who are on the national security career track.

We're also implementing an auditing practice that will include Department of Justice lawyers, inspectors in the FBI and FBI lawyers to go out and methodically audit the use of the national security letters.

More generally, we are going to create a compliance program within the bureau that will be interdisciplinary and it will make sure that not just with national security letters -- I mean, this is one tool, and it's a tool that, as indicated in this report, we need better controls on.

Our concern is that there may be other things that we need to make sure that we've got better controls on; that we think we've given perfectly clear guidance but, in terms of execution in the field, we've got some problems.

So again, I can't say enough that we take this report extremely seriously. We know we've got issues. We know we've got problems. The director and upper management is absolutely committed that we're going to fix this.

CONYERS: Time has expired.

GOHMERT: Thank you, Mr. Chairman.

CONYERS: Mr. Artur Davis from Alabama is recognized.

DAVIS: Thank you, Mr. Chairman.

Ms. Caproni, give me your best legal assessment: Will the exclusionary rule apply to any evidence obtained from the improper issuance of these letters?

CAPRONI: Probably not. But I haven't quite, frankly, given that a great deal of thought.

It's not a Fourth Amendment violation. Exclusionary rule clicks in usually when you've got a Fourth Amendment violation. These records are being held by third-party businesses. So it's not a...

DAVIS: Why would there not be Fourth Amendment implications if information was obtained as a result of the improper use of federal statutory authority?

CAPRONI: There would be other problems, but I don't think there's a Fourth Amendment problem.

DAVIS: Well, do you think that there would be a practical problem -- classic hypothetical -- if a national security letter was improperly issued and it turned out later on there were perhaps a valid basis for the issuance of a warrant? Wouldn't that possibly be compromised, or the emergence of a valid basis later on be compromised by the misuse of an NSL?

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

CAPRONI: Again, I'm always leery of responding to hypotheticals. All I can say is there's no -- we are not -- we're not minimizing this. We do not...

DAVIS: So you're not sure.

Let me follow up on Mr. Schiff's questions.

Are you familiar with the name Bassem Youssef?

CAPRONI: Yes, sir, I am.

DAVIS: And Mr. Youssef, as I understand it, was in charge of the Communications Analysis Unit at the bureau, is that right?

CAPRONI: He was, beginning in the spring of '05.

DAVIS: And is it accurate that Mr. Youssef raised concerns about the misuse of the NSLs to his superiors?

CAPRONI: That will have to be determined through the inspection. I do not know the answer to that question.

DAVIS: Well, you know that that's been reported. And I assume, Mr. Fine, neither you nor Ms. Caproni have any basis to dispute what Mr. Youssef's lawyers are saying about him making that report.

CAPRONI: I would note that Mr. Youssef is in litigation with the FBI.

DAVIS: That's not what I asked you. I asked you if you had any basis to dispute the report.

CAPRONI: I don't know one way or the other...

DAVIS: Mr. Fine, do you have a basis to dispute that there were complaints raised by the former head of the Communications Analysis Unit?

FINE: We didn't review what he did...

DAVIS: Mr. Fine, how is it possible that you did not review the fact that the former head of the unit raised questions about the misuse of the NSLs? How is it remotely possible that was not reviewed?

FINE: We reviewed what happened in that unit and what was issued. And we did review the discussions that occurred between the Office of General Counsel and...

DAVIS: Mr. Fine, if the head of the unit, not a secretary, not an intern, not a line officer, but the head of the unit raised concerns, how is it possible that you didn't conduct an interview of Mr. Youssef?

FINE: We did interview Mr. Youssef. And he did not -- we did not hear that concern from him. And, in fact, from the interview of Mr. Youssef, and also from the review of the records, we saw that he signed a letter. And many...

DAVIS: Are you disputing that Mr. Youssef complained about the improper issuance of NSLs?

FINE: To his superiors?

DAVIS: Yes.

FINE: I don't know that. I do know...

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

DAVIS: Did you ask him?

FINE: I don't believe -- I don't believe -- I'm not sure whether we asked that question.

DAVIS: Mr. Fine, how do you possibly not ask the head of the unit if he had any concerns about whether or not the statute was followed? How does that possibly not come up as a question?

FINE: We did ask him and we questioned him extensively, our attorneys did, about the communications between the Office of General...

DAVIS: Well, did he say that he raised questions?

FINE: Not that I'm told, no.

DAVIS: Not that you remember or not that you're told, which one?

FINE: Well, I actually didn't -- but let me just check.

DAVIS: And while you're working on the answer there, Mr. Fine, that rather obvious observation -- I hope that your time to get the answer is not taken out of my time -- if you have the head of the Communications Analysis Unit raising questions about how that unit does its work, it's a little bit amazing to me that you're having to search your memory as to what happened during the interview.

But let me move on.

FINE: Well, can...

DAVIS: Is it true that -- well, my time's limited, Mr. Fine -- is it true that Mr. Youssef won the Director of Central Intelligence Award in 1995 for his work infiltrating the group that tried to blow up the Trade Center in 1993?

FINE: I have heard that.

DAVIS: Do you have any reason to dispute it?

FINE: No.

DAVIS: Is it true that Mr. Youssef was the legal attache to Saudi Arabia during the time of the Khobar Towers bombing was being investigated?

FINE: I have no reason to dispute that.

DAVIS: Is it true that Mr. Youssef received outstanding personnel evaluations during the time?

FINE: I have no reason to dispute that.

DAVIS: So you have someone who was the head of a unit, who had won awards for his intelligence work, who apparently received superior evaluations, raising concerns about how his unit was being conducted, is that accurate?

FINE: No, I'm not sure it is accurate. I am...

DAVIS: What is inaccurate about it?

FINE: What is inaccurate is that it is not clear what concerns he raised and what he did to stop this. And we did look...

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

DAVIS: Well, again, Mr. Fine, how -- I know my time is up, but if the chair will indulge me one question -- I guess I'm searching for what is opaque about this. This gentleman was in a very important position. He was in charge of the unit.

You admit that you interviewed him, but your memory seems foggy as to what you asked him and your memory seems foggy as to whether or not he raised concerns to his superiors and what the concerns were.

I can't imagine a more important interview that you could have conducted.

FINE: We did conduct that interview, and we went over extensively what the concerns were between him and the General Counsel's Office and the attempts to put the exigent letters...

DAVIS: Who did he register his concerns with?

CONYERS: The gentleman's time has just about expired. What I'd like to do is give the inspector general an opportunity to fully finish his answer.

FINE: We did interview Mr. Youssef, Congressman. And we did not find that, as a result of his actions, that the problems were corrected.

We did find through review of the NSLs that he signed, one, that under his leadership these exigent letters continued, and we saw the efforts between the Office of General Counsel and the CAU to correct this, which did not occur. And we did not see that he put a stop to this.

However, we did not do...

DAVIS: Was he empowered to put a stop to it?

FINE: He was the head of the unit.

DAVIS: What if his superiors didn't consent?

CONYERS: Just a moment. If my colleague will suspend, I want him to be able to complete his answer before we go on to the next member.

FINE: We did not see that this practice was stopped during his time.

There was an attempt, to sort of, provide NSLs reasonably soon after the exigent letters. But the exigent letters continued. And it is important to determine who did what, when and how.

FINE: And the FBI's going to do that. And we are going to look at that very carefully as well.

But our review was not to look at everybody's actions up and down the line, including his or others', to determine what steps each one of them took. What we tried to do is present the problem and the issue and make sure that it stopped as a result of it.

CONYERS: The gentleman's time has expired.

The chair recognizes Darrell Issa, the gentleman from California.

ISSA: Thank you, Mr. Chairman.

I guess I'll start off slow and just follow up on Mr. Gohmert for a second.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

It does seem amazing that an organization of excellence, as the FBI has historically been, would adopt a "We've got you to the Peter principle achievement level" with this up-or-out policy.

And I would strongly second Mr. Gohmert's -- what I think he was saying, which is if you have people who can be very good at what they do at the beat level, so to speak, of the FBI, in various positions, if they can, in fact, be superb leaders at a level that they're comfortable, and, quite frankly, in a community that they're comfortable living and working in and building more capability, rapport and analysis capability, and you adopt an up-or-out program, what you do is, you force them either to leave because they don't want to leave communities they're attached to, or, quite frankly, you force them to a management level they may not be comfortable with.

It's bad enough that the Army will not allow a great company commander to continue being a company commander and must force them to a staff position somewhere where they endlessly see papers in the hopes that they someday will get a battalion command, but there's a certain amount of history there.

I strongly suggest that the FBI shouldn't have a history that people doing a good job at a given level be forced on.

ISSA: Having said that, that's a management decision that the next administration, hopefully, will straighten out.

But speaking of management decisions, Mr. Fine, I am -- or General Fine -- I'm a little shocked that, under this attorney general, this administration seems to look at violations of constitutional rights for limited capabilities that we have granted from this body as, as the general counsel said, troubling.

If what the FBI did was done by a private-sector individual, wouldn't the FBI be arresting them? Wouldn't the U.S. attorneys be prosecuting people who played fast and loose with these rules?

FINE: It depends on the intents involved and what happened.

ISSA: OK. Let me back up.

If there was a pattern over time, as there is, of abuses piling up to where it was clear that people knew it was happening, even some people clearly made comments that it shouldn't be happening, that it was inconsistent with the law, but it continued, isn't that a poster child for the FBI and the U.S. Attorney's Office criminally prosecuting people who do these things?

FINE: Again, if there was an intent to do that, as opposed to a pattern of negligence, and also a knowledge of this.

And we went in and looked at it after the fact and found all sorts of problems and compiled a 126-page report which lays it out in pretty black and white. And it is a serious, serious abuse.

But at the time, were they aware of it, did they know about that, and what their intent was -- that's much harder to say.

We did not find evidence of criminal misconduct, but we certainly found evidence...

ISSA: Well, wait a second. Wait a second.

Piling up evidence that crosses the guidance we allow to pile up that evidence, and you're saying that it's not criminal.

FINE: Well, you have to look at the individual allegations as well. We looked at the files. We found in many files that there were no abuses. We found in others that there were problems with them.

ISSA: But there are no prosecutions and no dismissals, is that correct?

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

FINE: Well, there are no prosecutions.

The FBI is looking at the evidence right now to see what people knew and what they did. Whether it was because of any intentional conduct that they knew they were doing wrong, we didn't see that. But we didn't do a review where we asked each individual, "What did you do and why?" we did a review of an audit of this to lay out the problems for the Congress.

ISSA: Well, I would suspect that I join the chairman and many members on both sides of the aisle in saying I have serious doubts about whether or not the Congress can continue to extend capabilities that are not 100 percent adhered to and there are no significant results when they're not adhered to, and then not feel that what we're doing is giving the FBI the ability to violate people's constitutional rights.

And, you know, I heard today, "Well, geez, we wouldn't exclude this" --and Congressman Schiff brought it out -- "we won't exclude this information, even though we played fast and loose. And we won't dismiss and we won't prosecute."

Well, with all due respect, from the attorney general on down, you should be ashamed of yourself.

We stretched what we could give in the Patriot Act. We stretched to try to give you the tools necessary to make America safe. And it is very, very clear that you've abused that trust.

And when the reauthorization of the Patriot Act comes up or any bill coming down the pike, if you lose some of these tools, America may be less safe, but the Constitution will be more secure. And it will be because of your failure to deal with this in a serious fashion.

I yield back.

CONYERS: Thank you very much.

The chair recognizes Keith Ellison, the gentleman from Minnesota.

ELLISON: Thank you, Mr. Chair.

Mr. Fine, I want to talk to you about your report recommendations, starting with the exigent letters.

Wouldn't it be better, simply, to adopt the FBI's current practice of simply banning the use of exigent letters? I noticed that in your recommendations -- or in what I believe are your recommendations -- your suggestion is to take steps that the FBI not improperly use the letters. But why not just say: "No exigent letters"?

FINE: Well, there shouldn't be an exigent letter of the sort that they use. There is a process under the statute to get emergency information under certain conditions. And that's the way they ought to do it. So that is a proper use of such a request.

They surely should ban the way they did it in the past.

ELLISON: And that would be a change by statute or a rule change?

FINE: Well, it doesn't need to be a statute. There is a statute that allows voluntary disclosure if there is an imminent threat and danger to the safety of an individual or others.

And if there is that exigent circumstance, they can get the information and should use such a letter.

But what they shouldn't do is combine it with an NSL, the way they did in the past. They ought to completely

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

separate that and follow the statute..

ELLISON: Right.

So what you're saying is that if the practice in which the FBI was using the exigent letters combined with the NSL, if the statute were properly followed, then there wouldn't be the problem that we see today, is that right?

FINE: That's correct.

ELLISON: Now, what sort of sanctions do you think should be applied, given the way that the FBI did use the NSL and the exigent letters?

FINE: I think the FBI ought to look at this and look at the individuals involved and find out if they inappropriately and knowingly misused the authorities. They ought to take appropriate action against individuals, either management individuals who allowed it to occur or individuals in the field. And if they had poor performance, that ought to be assessed as well.

So I think that ought to be something that the FBI is looking at. But I don't think they ought to say, simply because there was a misuse of the statute inadvertently, that that would necessarily require misconduct charges against them.

ELLISON: Right.

Well, you know, part of the problem here is the very nature of the act that allows for the expanded use of the NSL is below the radar; it's not subjected to neutral.

And so it by nature lacks transparency, which is why people are so upset that the abuses took place.

But I guess my next question is -- another recommendation that you have made is that there be greater control files for the NSLs. How would you envision that working?

FINE: There should be greater controls on the use of NSLs. They ought to make sure that the people know when they can be used and under what statute they can be used. There need to be signed copies of the NSLs so that there can be an audit trail. They have to be connected to an investigative file, not a control file.

ELLISON: Excuse me -- I'm sorry, Mr. Fine. Do you see this as essentially a training problem?

FINE: I think it's a training problem. I think it's a supervision problem. I think it's an oversight problem. And I think it's a lack of adequate internal controls in auditing problem as well.

ELLISON: Now, that brings me to a few questions I had for Ms. Caproni.

Ms. Caproni, do you have a staff to make all the changes that are needed in order to have this program work properly?

CAPRONI: I would always like more resources.

ELLISON: No, I'm asking you -- that's not my point.

My question is: In order to -- we could just simply go back to the status quo ante, back to the pre-Patriot Act, where NSLs were authorized but not the expanded use of them that we have now. That could be one way to simply solve this problem.

But my question is: At this time, do you have the staff to provide the training, provide the controls that are called for by the recommendations?

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

CAPRONI: I do. We're going to get some more staff that we've already discussed. We're going to get some more analytic help, because we think that some of this would have been detected if we had had good analytic help so that we could see trends.

But I think that we have enough lawyers. I think we can do what needs to be done. We're going to have assistance from Department of Justice lawyers for some of this, but I think we have sufficient resources.

ELLISON: Ms. Caproni? If you have the sufficient resources, why didn't you use them before?

ELLISON: I mean, I guess the question that comes up in my mind is that you either don't have the resources to effectuate the changes that have been recommended, or you do; and if you do, why weren't they applied?

CAPRONI: This report told us a lot that we just didn't now. I mean, I will fall on that sword again, which is, we learned a lot from this report, and we're going to make changes.

I think I've got the personnel to do it. I think we've got the resources. We're going to make the resources available. This is important to us. It is important to us to regain the confidence of the American people and to regain the confidence of this committee. You're one of our oversight committees and you're very important to us.

So we're not -- trust me, I'm not happy that we have this report and that I'm in a position of saying, you know, we failed.

ELLISON: Excuse me, Ms. Caproni, if I could just go back to Mr. Fine.

Mr. Fine, one of the changes that was made in the Patriot Act was to say, I think, people other than headquarters officials could issue these letters.

Should the authority for issuance of the letters be retracted to what it was before the Patriot Act?

FINE: I'm not sure of that, and I don't want to necessarily give legislation that should occur.

I do think it's important, if that authority is out there, that it has to be overseen.

And bringing things back to headquarters may or may not be the answer. As you recall in the September 11th attacks with the Moussaoui case, one of the concerns was headquarters was controlling the field too much.

And so, there are considerations on both sides of this issue. I do think that when it does go out there, it has to be used appropriately and overseen appropriately.

ELLISON: But if you had a narrower route through which these letters were authorized, wouldn't you have greater accountability?

FINE: You could. You could have greater accountability. On the other hand, the effectiveness could be diminished significantly.

So I think that's the balance that has to be struck, Congressman.

CONYERS: Time of the gentleman has expired.

But I would like to say to Mr. Ellison, he's raised the point that we need to try to figure out at this hearing: Are there in existence the resources that are required and needed to reveal all of these people who have been abused or violated by this system?

CONYERS: For this hearing to close down with the gentleman from California, Mr. Berman, who will be

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

recognized next, without us having figured out, for example, that we don't have anywhere near the resources, as I've been talking with the gentleman from California, Mr. Lungren, about, either in the Federal Bureau of Investigation or in the Office of the Inspector General.

If resources don't exist here, we may end up very well correcting everything from this point on, but how many thousands of people will have been violated that will -- we'll all be saying from now on, "Not to worry. It's all over with."

And that is a troubling consideration, Mr. Lungren, that we've had under discussion, that I'm still looking for the answer to.

So I recognize the gentleman from California, Mr. Berman.

BERMAN: Thank you very much, Mr. Chairman.

Mr. Fine, Section 126 (a) of the Patriot Act requires that not later than one year after the date of enactment of this act, the attorney general shall submit to Congress a report on any initiative of the Department of Justice that uses or is intended to develop pattern-based data mining technology.

The one-year deadline expired March 9th of this year. To my knowledge, we haven't received this report. Can you give us an update on the progress of this report?

FINE: From the attorney general? No, I don't -- I can't give you progress. That's not my office.

But I certainly can bring back that question to the department.

BERMAN: But I thought...

CAPRONI: Congressman, I, unfortunately, can tell you. Yes, it was not submitted on time. I think we sent a letter indicating that. It's still being worked on. I saw a draft going back across between us and DOJ. So it's being worked on.

BERMAN: OK, well, then, let me ask you: As I understand the audit that the inspector general has undertaken, information from the national security letters is routinely added to the FBI's internal automated case system, which has about 34,000 authorized users, and then, is periodically downloaded into the investigative data warehouse, which has approximately 12,000 users.

Is it possible that other agencies of the federal government or anywhere are using information in that investigative data warehouse for data mining purposes?

CAPRONI: For data mining purposes -- I don't know the answer to that.

I mean, they could get access to it as appropriate for their agency.

BERMAN: So it is possible.

CAPRONI: I don't know the answer. I don't know.

BERMAN: You don't know if it's possible or you don't know if they are?

CAPRONI: I don't know what they're doing with it. And I don't know what rule and restrictions govern them, so I just can't answer that question.

BERMAN: Well, let me get one thing clear. Maybe I'm under -- is the report that we are awaiting an inspector general's report or an attorney general's report?

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

CAPRONI: It's attorney general.

BERMAN: Attorney general's report. All right.

So will that report include data mining of information in the investigative data warehouse by agencies not within the Justice Department -- this report that you've seen circulating, will it include data mining of information by other agencies from the Justice Department's Investigative Data Warehouse?

CAPRONI: No, it does not. But I don't know whether that means that no such that no such activities are occurring or because it's not within the scope of the request.

BERMAN: Well, we think -- since I was involved in this language -- we think that since the database is under the purview of the Department of Justice, use of it by other agencies would be included in that report, under Section 126(a).

CAPRONI: I will make sure that the people at DOJ understand that that's your interpretation of it. I just, unfortunately, I've been in the world of NSL and this report, and I haven't been in the world of the data mining report, so I just haven't read it. So that's why I can't answer your question.

BERMAN: So you have not been personally involved, then, in determining whether other agencies are being cooperative on how they're using the data from the IDW. I take it you don't...

CAPRONI: I have not. I just haven't been involved in it.

BERMAN: If you, subsequent to this hearing, could get that information and pass it on to me, I'd be very grateful.

CAPRONI: Certainly...

BERMAN: The information about whether the report will talk about other agencies' use of the Justice Department's Investigative Data Warehouse for data mining purposes.

CAPRONI: Again, I will make sure that the department understands your position.

BERMAN: Thank you.

(UNKNOWN): Will the gentleman yield to me?

BERMAN: I'd be happy to.

(UNKNOWN): To ask a question.

Ms. Caproni, one question just came to my mind, and that is, part of this testimony today has talked about how agents in the field and special agents in charge in the field didn't get the proper legal advice from, I presume, people that report to you, that they were not challenged as to the legal sufficiency of the NSLs or the exigent letters.

Is that correct?

CAPRONI: Let me -- I think that comment was relative to the lawyers in the field who actually do not report to me.

(UNKNOWN): Who do they report to?

CAPRONI: They report to the special agents in charge.

They report to their field office head. That's one of the things that Mr. Fine has suggested that we look at, and that is actively under discussion at the bureau right now, whether that reporting structure should change.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

(UNKNOWN): So they don't report to you at all?

CAPRONI: No, sir, they do not.

(UNKNOWN): So they were on their own in the advice they were giving of a legal nature to the agents and the special agents in charge to whom they report.

CAPRONI: On a reporting basis, they do not report to me. I do not supervise them. I am in charge of the legal program. So we provide the CDCs -- that's their title -- we provide them with substantial legal advice, and they frequently call us when they have questions. But I do not rate them, and they do not report to me.

I don't hire them; I don't fire them.

(UNKNOWN): I know, but what I'm trying to figure out is if these attorneys report to the SAC, does that make it more difficult for them to tell the SAC that he or she's wrong when they're asking for one of these letters?

CAPRONI: That's the concern that Mr. Fine has raised. I mean, I...

(UNKNOWN): Well, do you share that concern?

CAPRONI: I do share that concern.

(UNKNOWN): And could that be one of the real problems we've got here?

CAPRONI: I will say there are arguments both ways, Congressman. It is not -- and the reason I say that is because I report to the director of the FBI, and I don't have any problem telling the director of the FBI my legal advice. And if he doesn't like it, it's still my legal advice. That's what the CDCs should be doing. But whether they...

(UNKNOWN): But at least my experience has been SACs are pretty important people in their various offices and most people generally think they're the top dog. And we have this problem where, apparently, good legal advice either was not given or not accepted, and maybe that is something we ought to look at, if you folks won't look at it.

CAPRONI: Again, we are actively looking at that very question, of whether the CDC reporting structure should change.

(UNKNOWN): And I thank the gentleman from California for yielding, although he's not here to receive it back.

CONYERS: I thank you all.

The gentleman from Minnesota had one last question that I've agreed to entertain, if you will.

ELLISON: Thank you, Mr. Chair.

My question is, of all the letters that have been issued and all the inaccurate and improper data that has been sent forth, clearly some information came back. And in the cases where individual's information was obtained in violation of the rules and statutes, what has happened? Have these individuals been notified? What recourse do they have? What's the story on the people?

CAPRONI: The people are not notified. The records are removed from our databases and the records are destroyed.

FINE: That's correct.

CONYERS: Thank you very much.

REP. JOHN CONYERS JR. HOLDS A HEARING ON FBI PATRIOT ACT MISUSE CQ Transcriptions" All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmi

Ladies and gentlemen, this has been an excellent hearing. We thank the witnesses for a continued and extended period of examination. We'll all be working together.

There are five legislative days in which members may submit additional questions to you, and send them back as soon as you can.

CONYERS: We also want to enter into the record Caroline Fredrickson's statement on behalf of the American Civil Liberties Union; Congressman Coble's Department of Justice fact sheet release.

We also have the New York Times, which officially alerted FBI to rules abuse two years ago, dated March 18. And we also have a letter being hand-delivered to the general counsel, dated today, March 20th, which asks her for additional information.

The record will be open for five additional days. And without any further business before the committee, the hearing is adjourned. We thank you for your attendance.

END

NOTES:

[????] - Indicates Speaker Unknown

[--] - Indicates could not make out what was being said.[off mike] - Indicates could not make out what was being said.

LOAD-DATE: March 20, 2007

EXHIBIT “II”

A Review of the Federal Bureau of Investigation's Use of National Security Letters



Office of the Inspector General
March 2007

UNCLASSIFIED

CHAPTER ONE INTRODUCTION

In the Patriot Reauthorization Act, enacted in 2006, Congress directed the Department of Justice (Department) Office of the Inspector General (OIG) to review “the effectiveness and use, including any improper or illegal use, of national security letters issued by the Department of Justice.”¹ The Act required the OIG to conduct reviews of the use of national security letters for two separate time periods.² This report describes the results of the first OIG review of the FBI’s use of national security letters (NSLs), covering calendar years (CY) 2003 through 2005.³

I. Provisions of the USA Patriot Act and Reauthorization Act

In October 2001, in the wake of the September 11 terrorist attacks, Congress passed the USA PATRIOT Act.⁴ Section 505 of the Patriot Act expanded four existing statutes (the “national security letter statutes”) that authorized the Federal Bureau of Investigation (FBI) to use national security letters to obtain certain specified types of information from third parties for use in authorized counterintelligence, counterterrorism, and foreign computer intrusion cyber investigations. As part of the Patriot Act legislation, Congress enacted a fifth NSL authority permitting the FBI to use national security letters to obtain consumer full credit reports in international terrorism investigations.

National security letters, which are written directives to provide information, are issued by the FBI directly to third parties, such as telephone companies, financial institutions, Internet service providers, and consumer credit agencies, without judicial review. In these letters, the FBI

¹ USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 119(a), 120 Stat. 192 (2006) (Patriot Reauthorization Act).

² Although the Act only required the OIG to include calendar years 2003 through 2004 in the first report, we elected to also include 2005 in this first report. The second report, which is due to Congress on December 31, 2007, will cover calendar year 2006.

³ The Patriot Reauthorization Act also directed the OIG to conduct reviews on the use and effectiveness of Section 215 orders for business records, another investigative authority that was expanded by the Patriot Act. The OIG’s first report on the use and effectiveness of Section 215 orders is contained in a separate report issued in conjunction with this review of NSLs.

⁴ The term “USA PATRIOT Act” is an acronym for the law entitled the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001). This law is commonly referred to as “the Patriot Act.”

can direct third parties to provide customer account information and transactional records, such as telephone toll billing records.⁵

The national security letter authorities expanded by the Patriot Act were originally scheduled to sunset on December 31, 2005, but were temporarily extended by Congress until it finalized a reauthorization bill. Congress passed the reauthorization bill in early 2006, and on March 9, 2006, the President signed into law the Patriot Reauthorization Act, which, among other things, reauthorized the five national security letter authorities.

In the Patriot Reauthorization Act, Congress directed the OIG's review to include:

- (1) an examination of the use of national security letters by the Department of Justice during calendar years 2003 through 2006;
- (2) a description of any noteworthy facts or circumstances relating to such use, including any improper or illegal use of such authority; and
- (3) an examination of the effectiveness of national security letters as an investigative tool, including –
 - (A) the importance of the information acquired by the Department of Justice to the intelligence activities of the Department of Justice or to any other department or agency of the Federal Government;
 - (B) the manner in which such information is collected, retained, analyzed, and disseminated by the Department of Justice, including any direct access to such information (such as access to “raw data”) provided to any other department, agency, or instrumentality of Federal, State, local, or tribal governments or any private sector entity;
 - (C) whether, and how often, the Department of Justice utilized such information to produce an analytical intelligence product for distribution within the Department of Justice, to the intelligence community . . . , or to other Federal, State, local, or tribal government departments, agencies or instrumentalities;

⁵ The statutes do not authorize the FBI to collect the content of telephone calls and e-mail. For that information, the FBI must obtain court approval or voluntary production of the records pursuant to 18 U.S.C. § 2702(b)(8) (2000).

counterintelligence cases. Before the Patriot Act, the FBI could issue RFPA NSLs upon certification of

specific and articulable facts giving reason to believe that the customer or entity whose records are sought is a foreign power or an agent of a foreign power. . . .²¹

Since the Patriot Act, the FBI may obtain financial records upon certification that the information is sought

for foreign counterintelligence purposes 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 to the Constitution of the United States.²²

In December 2003, Congress amended the RFPA to expand the definition of “financial institutions” to which NSLs could be issued, including entities such as rental car companies, automobile dealerships, credit unions, issuers of travelers’ checks, pawnbrokers, and real estate companies.²³

The FBI can disseminate information derived from the RFPA national security letters only in accordance with the Attorney General Guidelines governing national security investigations and can disseminate such information to other federal agencies only if the information is clearly relevant to the authorized responsibilities of those federal agencies.²⁴

B. The Electronic Communications Privacy Act

In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA), which extended statutory protection to electronic and wire communications stored by third parties such as telephone companies and Internet Service Providers.²⁵ The statute restricted the government’s access to live telephone transactional data, such as the telephone numbers that a particular telephone number calls or received (known as “pen register” and

²¹ 12 U.S.C. § 3414(a)(5)(A) (2000).

²² 12 U.S.C. § 3414(a)(5)(A) (2000 & Supp. IV 2005). Financial records accessible to the FBI under the RFPA were also subject to compulsory process through subpoenas, search warrants, and formal requests, all of which, with limited exceptions, required notice to the customer.

²³ See 12 U.S.C. § 3414(d) (2000 & Supp. IV 2005), as amended by the Intelligence Authorization Act for Fiscal Year 2004, Pub. L. No. 108-77, § 374(a) (2004), which incorporated the definition of “financial institution” set forth in 31 U.S.C. §§ 5312(a)(2) and (c)(1).

²⁴ 12 U.S.C. § 3414(a)(5)(B) (2000).

²⁵ 18 U.S.C. § 2709 (1988).

“trap and trace” data). The ECPA required the government to obtain a court order for which it must certify the relevance of the information to an ongoing criminal investigation.²⁶ The statute requires that subjects of government requests for these records be given advance notice of the requested disclosure and an opportunity to challenge the request.

However, the ECPA allowed the FBI to obtain “subscriber information and toll billing records information, or electronic communication transactional records” from a “wire or electronic communications service provider” in conjunction with a foreign counterintelligence investigation. Before the Patriot Act, the FBI could obtain ECPA NSLs upon certification of

specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power. . . .²⁷

Since the Patriot Act, the FBI must certify that the information sought 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 on activities protected by the first amendment to the Constitution of the United States.²⁸

In 1993, Congress expanded the ECPA NSL authority by permitting access to the subscriber and toll billing records of additional persons, such as those who were in contact with agents of a foreign power.²⁹ Congress amended the ECPA again in 1996 by defining “toll billing records” to expressly include “local and long distance toll billing records.”³⁰

Recipients of ECPA NSLs were prohibited until the Patriot Reauthorization Act from disclosing to any person that the FBI had sought or obtained the requested information.³¹

²⁶ A “pen register” is a device that records the numbers that a target telephone is dialing. A “trap and trace” device captures the telephone numbers that dial a target telephone. See 18 U.S.C. § 3127 (2000).

²⁷ 18 U.S.C. § 2709(b)(1)(B) (2000).

²⁸ 18 U.S.C. § 2709(b)(2) (2000 & Supp. IV 2005).

²⁹ Pub. L. No. 103-142, § 2, 107 Stat. 1491 (1993). The 1993 amendment also provided additional congressional reporting requirements. *Id.*

³⁰ Intelligence Authorization Act for Fiscal Year 1997, Pub. L. No. 104-293, § 601(a), 110 Stat. 3461 (1996).

³¹ 18 U.S.C. § 2709(c) (2000).

CHAPTER THREE

THE FBI'S COLLECTION AND RETENTION OF INFORMATION OBTAINED FROM NATIONAL SECURITY LETTERS

In this chapter we describe the process by which FBI agents obtain approval to issue national security letters. We also describe the manner in which the FBI obtains information through national security letters from third parties and retains such information in FBI Headquarters and field divisions.

I. The FBI's Process for Collecting Information Through National Security Letters

According to our interviews of FBI personnel, case agents conducting counterintelligence, counterterrorism, or foreign computer intrusion cyber investigations who need telephone or e-mail transactional activity, subscriber information, financial transactions, or credit information relevant to their investigations first assess the most effective investigative technique available at a particular stage of the investigation. For example, if the facts developed indicate a nexus to possible criminal activity, agents can ask the United States Attorney's Office to open a grand jury investigation, which allows prosecutors to issue federal grand jury subpoenas to obtain third party records.⁵⁰ If there is a criminal nexus, prosecutors often prefer to use grand jury subpoenas because they generally can obtain grand jury subpoenas quickly and recipients respond more promptly to grand jury subpoenas than they do to NSLs. However, issuance of a grand jury subpoena risks public disclosure that the government is conducting a national security investigation. As a result, agents often consider alternative investigative techniques, such as national security letters, which avoid public disclosure of the existence of an investigation.

To obtain approval within the FBI to issue national security letters, FBI agents must determine that information available pursuant to one of the national security letter authorities is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities and, with respect to an investigation involving a "U.S. person," is "not solely conducted on the basis of activities protected by the First Amendment."⁵¹ Case agents assigned to counterterrorism, counterintelligence, or cyber squads are responsible for preparing the

⁵⁰ Terrorism investigations often have a potential criminal nexus under statutes proscribing material support of terrorism and conspiracy, and federal statutes criminalizing threats against public facilities, aircraft, and other transportation systems, as well as possession of weapons of mass destruction.

⁵¹ 18 U.S.C. §§ 2709(b)(1) and 2709(b)(2); 12 U.S.C. § 3414 (a)(5)(A); 15 U.S.C. § 1681u(a); 15 U.S.C. § 1681v(a).

documentation necessary to secure approval to issue a national security letter. Case agents are encouraged to check FBI databases, such as the Automated Case Support (ACS) system and Telephone Applications, a specialized application storing telephone record data, to determine whether the information they need has previously been obtained by the FBI or is available through public search engines or commercial databases.

FBI administrative policy, set forth in the partially classified National Foreign Intelligence Program (NFIP) Manual and on NSLB's Intranet website, requires that case agents prepare two documents to obtain an NSL: (1) an electronic communication (EC) seeking supervisory approval for the national security letter and (2) the national security letter itself.

1. Electronic Communication (Approval EC)

The EC used to obtain approval of national security letters serves four functions. It:

- documents the predication for the national security letter by stating why the information was relevant to an authorized investigation;
- documents the approval of the national security letter by appropriate personnel;
- includes information needed to fulfill congressional reporting requirements; and
- transmits copies of the request to the FBI-OGC; FBI Headquarters Counterterrorism, Counterintelligence, or Cyber Division; and, when the recipient is not located in the field division issuing the national security letter, the field division that is asked to serve the national security letter.

During the period covered by our review, NSLB attorneys developed eight standard formats for the approval ECs that included routine elements common to all NSL requests, data elements needed for congressional reporting, and descriptions of the elements that were to be included in the national security letter package. NSLB modified the standard formats as national security letter statutes were revised and internal FBI administrative policy changed.

As discussed in Chapter Two, the Patriot Act lowered the predication standard for national security letters from "specific and articulable facts giving reasons to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power" to "relevan[ce] to an authorized investigation to protect against international terrorism or clandestine intelligence activities." The standard form used during the period covered by this review required that case agents provide

justification for opening or maintaining the investigation and “briefly state the relevance of the requested records to the investigation.”⁵²

To enable the FBI to collect data for its semiannual congressional reporting requirements, the following information also is required to be included in the approval EC: (1) for RFPA financial record NSLs, ECPA toll billing and electronic communication transactional records NSLs, and FCRA NSLs, the investigative subject’s status as a “U.S. person” or “non-U.S. person”; (2) the type of national security letter issued; and (3) a list of the individual telephone numbers, e-mail addresses, account numbers, or other records for which information is sought.⁵³

For field division-initiated national security letters, the Supervisory Special Agent of the case agent’s squad, the Chief Division Counsel, and the Assistant Special Agent in Charge are responsible for reviewing the approval EC and the national security letter prior to approval by the Special Agent in Charge. Division Counsel are required to review the national security letters to ensure their legal sufficiency – specifically, the relevance of the information requested to an authorized national security investigation.

The final step in the approval process occurs when the Special Agent in Charge or authorized FBI Headquarters official (the certifying official) initials the approval EC and signs the national security letter.⁵⁴ For national security letters generated by Headquarters, there is a parallel requirement for generating the approval paperwork for the signature of specially designated Headquarters officials.⁵⁵ Accordingly, the approval EC includes an “approved by” section that reflects the names of the reviewing

⁵² We discuss in Chapter Seven the circumstances that led to a February 2006 modification of models for NSL approval ECs, which now require a “full explanation of the justification for opening and maintaining the investigation of the subject” and to “fully state the relevance of the requested records to the investigation.”

⁵³ For purposes of the reporting requirement, a “United States person” is defined as a citizen of the United States, an alien lawfully admitted for permanent residence . . . , an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States”

⁵⁴ 50 U.S.C. § 1801(i). The congressional reporting requirements are described in Chapter Four.

⁵⁵ Certifying officials are not authorized to further delegate signature authority. Accordingly, Acting Special Agents in Charge are not authorized to sign national security letters.

⁵⁶ While NSLB encourages Headquarters operating divisions to utilize the NSLB Deputy General Counsel as the authorizing official, they are not required to do so. However, a legal review through NSLB is required.

and approving officials, who enter their initials on the hard copy of the document.

Field personnel in the four field offices we visited during the review told us that it takes from two to five days to obtain approval to issue NSLs. However, if there is no Special Agent in Charge in place in a field office, NSLs must be sent to another field office for approval by another Special Agent in Charge. Several Special Agents in Charge and Acting Special Agents in Charge told us that this has led to delays of as long as two weeks in securing approval to issue NSLs.

The approval EC also includes directions, known in FBI parlance as “leads,” to other FBI offices for actions that these offices are directed to take regarding the national security letter. Leads are “set” electronically through the FBI’s ACS computer system when the approval ECs are uploaded into the system. FBI personnel are responsible for checking ACS periodically to determine whether leads have been assigned to them. Leads also may be sent in hard copy via the FBI’s interoffice mail delivery system. The initiating field office also includes a lead to NSLB that instructs it to record the appropriate information needed to fulfill congressional reporting requirements and an informational lead notifying the Counterterrorism, Counterintelligence, or Cyber Division of the national security letter.

A case agent from the field office squad initiating the national security letter (the “office of origin”) hand carries the letter to the designated recipient if it is located in the field division. If the NSL recipient is located in another field division, the office of origin sets a lead to the field office where the recipient is located with instructions to personally deliver the national security letter to the recipient.

2. The National Security Letter

A national security letter is the operative document that directs a third party to provide specific records. Although the internal documentation supporting the approval of national security letters is classified, neither the letters themselves nor the information provided to the FBI in response to the letters is classified.

As mentioned previously, during the period covered by our review NSLB developed and posted on its Intranet web site eight standard formats or models for the different types of national security letters that request the following categories of information, each of which was derived from one of the four statutory national security letter authorities in the Electronic Communications Privacy Act (items 1 – 4), the Right to Financial Privacy Act (item 5), or the Fair Credit Reporting Act (items 6, 7 and 8):

1. Telephone subscriber information;
2. Telephone toll billing records;
3. Electronic (e-mail) subscriber information;

use certain delivery services to deliver national security letters, such as the U.S. Postal Service or restricted delivery options offered by private delivery services.⁵⁶

Some FBI agents complained to NSLB that failure to designate a due date or “return date” in the body of the NSL led to delayed responses by some recipients, which sometimes compromised time-sensitive investigations. NSLB concluded that there was no legal restriction against including a return date (much as a grand jury subpoena or administrative subpoena includes a specified “return date”).

Headquarters and field personnel in the four field divisions we visited told us that there is no FBI policy or directive requiring the retention of signed copies of national security letters or any requirement to upload national security letters into ACS. We found that the FBI has no uniform system for tracking responses to national security letters, either manually or electronically.⁵⁷ Instead, individual case agents are responsible for following up with NSL recipients to ensure timely and complete responses. Case agents are also responsible for ensuring that the documents or electronic media provided to the FBI match the requests, both as to content and time period; analyzing the responses; and, depending upon the type of records, providing the documents or other materials to FBI intelligence or financial analysts who also analyze the information received.

II. The FBI’s Retention of Information Obtained from National Security Letters

FBI case agents who obtain information from national security letters retain the information in different ways and in a variety of formats. The FBI has not issued general guidance regarding the retention of this information. The manner in which case agents retain the information depends upon the NSL type, the size and format of the response, and the manner in which the data is to be analyzed.

The case agents and squad supervisors we interviewed told us that they prefer to receive responses in electronic format for ease of storage and analysis. However, case agents and squad supervisors told us that the majority of the responses to all types of national security letters during the

⁵⁶ See EC from FBI-OGC to All Field Offices, *Legal Advice and Opinions; Service of National Security Letters* (June 29, 2005). The recipient could return responsive documents to the FBI via the same method. However, FBI personnel in the field offices we visited told us that the national security letters and responsive documents were usually personally delivered.

⁵⁷ In one field office we visited, the Special Agent in Charge maintains a control file with copies of signed national security letters, but this does not serve as a tracking system for responses.

period covered by our review were delivered in hard copies.⁵⁸ Field personnel told us that some major telephone companies provide telephone toll billing records and subscriber information in electronic format.

After inventorying the hard copy response to confirm that the information received matches the information requested in the NSL, the case agents generally prepare and upload an EC into ACS that documents receipt of the information. If the responsive records are relatively small in volume, the records are placed in the investigative case file or in a sub-file created to store information derived from NSLs. If the response to the NSL is voluminous, such as hundreds of pages of toll billing records or bank records, the documents are placed in centralized storage and the case agent completes a tracking form noting where the data is located.

If the response to the NSL is in an electronic format, such as a computer diskette, either the case agent or analyst initially reviews the response to confirm that the response matches the request and prepares the EC documenting receipt of the records. For example, the EC documenting receipt of ECPA telephone toll billing records or e-mail subscriber information states that the telephone number or e-mail address did or did not belong to the investigative subject or other target of the NSL. The case agent, data clerk, or analyst then provides the computer diskette or other electronic medium to an intelligence assistant or analyst, who is responsible for uploading the data into the pertinent database, such as the Telephone Applications database.⁵⁹

Once an EC is uploaded into ACS documenting receipt of the response to an NSL, authorized users of ACS may access the EC's contents. During the period covered by our review, there were approximately 29,000 authorized accounts issued for FBI personnel permitting them to access ACS, and approximately 5,000 accounts issued for non-FBI personnel.⁶⁰ The vast majority of the non-FBI account holders were officers serving on task forces, such as the Joint Terrorism Task Forces, the Foreign Terrorist Tracking Task Force, and the National Joint Terrorism Task Force. The remaining accounts were provided to staff in organizations such as the

⁵⁸ FBI officials told us that some of the smaller communication providers and Internet service providers furnish NSL data in hard copy form. This placed a significant burden on FBI support personnel who sometimes were required to manually enter the data into a word processing program for uploading and analysis.

⁵⁹ Telephone Applications contains raw data derived from NSLs, known as "metadata," including the call duration. It does not store the contents of telephone conversations. During the period covered by our review, approximately 17,000 FBI personnel and approximately 2,000 non-FBI personnel had accounts permitting them to access the FBI's specialized application for telephone record data.

⁶⁰ Case agents may restrict FBI and non-FBI personnel from accessing certain electronic files in ACS and other databases in highly sensitive cases.

Department of Homeland Security, the Terrorist Screening Center, and the National Counterterrorism Center.

Raw data derived from national security letters or the analysis developed from the raw data are often used to create spreadsheets that are stored on the computer hard drives of Headquarters or field office personnel. As we discuss in Chapter Five, case agents and analysts told us that they generate these types of spreadsheets to establish communication and financial networks between investigative subjects and others. In addition, Headquarters and field offices have shared or “networked” computer drives that permit all case agents, analysts, and support personnel on a particular squad or a larger universe of users in the field office or Headquarters division to access them. In such cases, raw NSL data or the analytical products derived from this data are retained on these shared drives.

If a field or Headquarters supervisor determines that a more formal analytical intelligence product, such as an Intelligence Information Report or Intelligence Bulletin, should use information from NSLs and be shared with other members of the intelligence community or others, analysts on the field-based Field Intelligence Groups or the Headquarters Directorate of Intelligence prepare these products.⁶¹ Electronic versions of these products are stored on field and Headquarters hard drives and, if a decision is made by the Directorate of Intelligence to disseminate them, are uploaded into the databases that are accessed by FBI and non-FBI personnel with authorized accounts.

We learned that the FBI’s retention practices regarding information received in response to NSLs in excess of what was requested, whether due to FBI or third-party error, varies. If a field case agent determines that the NSL recipient provided more information than was requested, the case agent is responsible for notifying the Chief Division Counsel (CDC) and sequestering the information. However, we found that FBI-OGC did not issue guidance to all CDCs as to the mechanics of sequestering this information until November 2005. Instead, FBI-OGC provided ad hoc guidance to field agents or Division Counsel who contacted FBI Headquarters with questions.⁶²

In our review, we learned of instances in which the excess records were destroyed, returned to the NSL recipient, or sequestered and given to

⁶¹ In Chapter Five, we describe how information derived from national security letters is used in the development of these intelligence products.

⁶² Eventually, in November 2006 NSLB sent guidance to the field that outlined the steps to be taken in these circumstances. The guidance memorandum stated that the agent should send the information to the CDC for sequestering, pending resolution of the matter. The memorandum also stated that NSLB would determine whether the sequestered information must be destroyed, returned to the provider, or may be used by the FBI, and whether the matter is reportable to the IOB.

the Chief Division Counsel. However, in other instances we found that case agents retained the information and sought approval to issue a new NSL to cover the excess information. Case agents and supervisors in the four field offices we visited told us that information provided in excess of what was requested in the NSL was not uploaded into ACS or other FBI databases.⁶³

As noted above, the principal FBI databases that contain raw data derived from national security letters are ACS and a specialized application for telephone data. ACS is the FBI's centralized case management system. NSL data is periodically downloaded from ACS and Telephone Applications into the FBI's Investigative Data Warehouse (IDW), a centralized repository for intelligence and investigative data with advanced search capabilities.⁶⁴ Raw data derived from national security letters also is retained in various classified databases operated by the FBI and other members of the intelligence community.

⁶³ We identified one instance in which the FBI uploaded into the Telephone Applications database data the FBI had improperly acquired in response to an ECPA NSL. We describe this matter in Chapter Six.

⁶⁴ According to the FBI, the Investigative Data Warehouse contains data from approximately 50 different FBI and other government agency databases and holds over 560 million records. The FBI estimated in December 2006 that approximately 12,000 FBI and non-FBI personnel have user accounts to access IDW, approximately 30 percent of which were issued to non-FBI personnel, such as Task Force Officers on the Joint Terrorism Task Forces (JTTFs). *FBI Oversight*: Hearing Before the Senate Comm. on the Judiciary, 109th Cong. 6 (2006) (statement of Robert S. Mueller, III, Director, Federal Bureau of Investigations).

The problems with the OGC database, including the loss of data from the OGC database because of a computer malfunction, also prevented us from determining with complete accuracy the number of investigations of different U.S. persons and different non-U.S. persons during which the FBI issued NSLs for financial records and NSLs for toll billing/electronic communication transactional records.

II. National Security Letter Requests From 2003 Through 2005

In this section, we describe the FBI's use of NSLs from 2003 through 2005 as documented in the OGC database. As discussed above, the data in the OGC database is not fully accurate or complete and, overall, significantly understates the number of FBI NSL requests. However, it is the only database that compiles information on the FBI's use of NSLs. Moreover, the data indicates the general levels and trends in the FBI's use of this investigative tool.

From 2003 through 2005, the FBI issued a total of 143,074 NSL requests (see Chart 4.1, next page).⁷⁴ Of that number, [REDACTED] requests (or [REDACTED] percent) were made pursuant to the three NSL statutes that are included in the Department's semiannual classified reports to Congress (RFPA, ECPA, and FCRAu). In addition, although the data was not required to be reported to Congress, the OGC database showed that the FBI issued [REDACTED] NSL requests for consumer full credit reports (FCRAv) during the same period. FBI records show that [REDACTED].

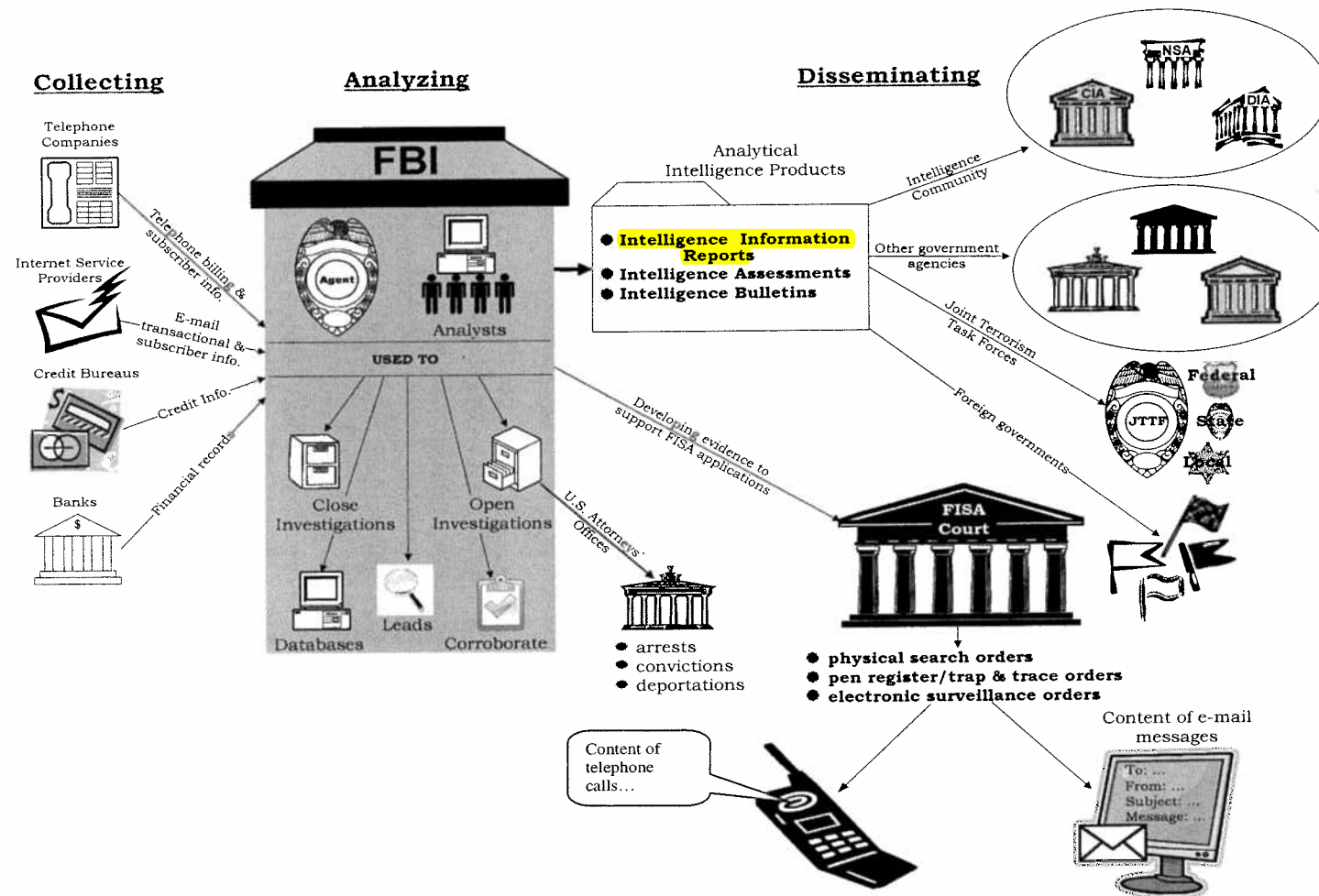
The number of ECPA NSL requests increased in CY 2004, and then decreased in CY 2005. We determined that the spike in CY 2004 occurred because of the issuance of 9 NSLs in one investigation that contained requests for subscriber information on a total of 11,100 separate telephone numbers. If those nine NSLs are excluded from CY 2004, the number of NSL requests would show a moderate, but steady increase over the three years.⁷⁵ The overwhelming majority of the NSL requests sought telephone toll billing records information, subscriber information (telephone or e-mail), or electronic communication transactional records under the ECPA NSL

⁷⁴ As noted earlier, we refer to the number of NSL requests rather than letters because one national security letter may include more than one "NSL request." See Chart 1.1 on page 4.

⁷⁵ The number of NSL requests we identified significantly exceeds the number reported in the first public annual report issued by the Department because the Department was not required to include all NSL requests in that report. The Department's public report stated that in CY 2005 the FBI issued 9,254 NSL requests for information relating to U.S. persons instead of the [REDACTED] NSL requests we identified because the public report did not include NSL requests under the ECPA for telephone and e-mail subscriber information, NSL requests under FCRAv for consumer full credit reports, or NSL requests related to "non-U.S. Persons."

DIAGRAM 5.1

How the FBI Uses National Security Letters



B. Analysis of Information Obtained From National Security Letters

The FBI performs various analyses and develops different types of analytical intelligence products using information from national security letters.

1. Types of Analysis

The review of information derived from national security letters is initially performed by the case agents who sought the national security letters. In counterterrorism investigations, once the case agents confirm that the response to the national security letter matches the request, the most important function of the initial analysis is to determine if the records link the investigative subjects or other individuals whose records are sought to suspected terrorists or terrorist groups. In counterintelligence investigations, the case agent's initial analysis focuses on the subject's network and, in technology export cases, the subject's access to prohibited technologies.

In some field offices, case agents are required to formally document their receipt of information from national security letters, including the date the information was received; the subject's name, address, and Social Security number; and a summary of the information obtained. This document then is electronically uploaded into the FBI's principal investigative database, the Automated Case Support (ACS) system. Once the data is available electronically, other case agents can query ACS to identify information obtained from national security letters that may pertain to their investigations.

After the case agent's initial analysis, analysts assigned to counterterrorism, counterintelligence, or cyber squads in the FBI's field divisions can use the NSL-derived information. The Counterterrorism and Counterintelligence Divisions in FBI Headquarters also conduct communication and financial analyses of NSL-derived information from different national security investigations.

Beginning in mid-2003, FBI field offices established Field Intelligence Groups (FIGs) as part of the Counterterrorism Division's Office of Intelligence. These squads later were moved to the FBI's Directorate of Intelligence. The FIG squads are staffed principally with intelligence analysts, language analysts, physical surveillance specialists, and field agents. FIG squads generate detailed analyses of intelligence information, some of which is derived from national security letters.

The FBI also evaluates the relationship between NSL-derived information and data derived from other investigative tools that are available in various databases. For example, when communication providers furnish telephone toll billing records and subscriber information on an investigative

subject in response to a national security letter, the data is uploaded into Telephone Applications, a specialized database that can be used to analyze the calling patterns of a subject's telephone number.

The FBI also places NSL-derived information into Investigative Data Warehouse (IDW), a database that enables users to access, among other data, biographical information, photographs, financial data, and physical location information for thousands of known and suspected terrorists. This FBI database contains over 560 million FBI and other agency records; information obtained from state, local and foreign law enforcement agencies; and open source data. The database can be accessed by nearly 12,000 users, including FBI agents and analysts and members of Joint Terrorism Task Forces.⁸⁷ Information derived from national security letters that is uploaded into ACS and into the Telephone Applications database is periodically uploaded to IDW.

FBI policy requires that case agents in counterterrorism investigations conduct a financial analysis of the investigative subject's financial activities. Some large FBI field divisions have dedicated squads, such as terrorist financing squads, to assist agents in analyzing the financial aspects of the subject. These squads may include specialists from outside of the FBI, such as the Defense Criminal Investigative Service or the Internal Revenue Service, who provide expertise in specific financial areas.

Like telephone call analysis, a review of financial records obtained through national security letters may show in a counterintelligence case that the subject is in contact with a foreign embassy or other foreign establishment or with other individuals known to be involved in intelligence activities. This analysis may reveal the names of people who have access to bank accounts, funds that have been transferred in and out of the accounts, and where the funds were transferred.

"Link analysis" is one of the principal analytical intelligence products generated by FIG analysts that rely on information derived from all types of national security letters used by the FBI during the period covered by our review. Link charts illustrate the telephone numbers, Internet e-mail addresses, businesses, credit card transactions, addresses, places of employment, banks, and other data derived from the NSLs, as well as information derived from other investigative tools and open sources. FBI agents and analysts develop link analyses in both counterterrorism and counterintelligence investigations, often integrating the results of multiple NSLs on the subjects of multiple FBI investigations.

Analytical intelligence products based on information obtained from national security letters integrate communication and financial information


⁸⁷ *FBI Oversight*: Hearing Before the Senate Comm. on the Judiciary, 109th Cong. 6 (2006) (statement of Robert S. Mueller, III, Director, Federal Bureau of Investigations).

on particular investigative subjects and their associates. For example, national security letter-derived data reflecting telephone activity on a cluster of dates may correspond with wire transfer information obtained from national security letters served on financial institutions. In one such example, this type of information was integrated to support investigations of a threat to a major U.S. city. FIG analysts combined related information from different investigations throughout the FBI to identify contacts and financial transactions between subjects of the investigation.

2. Formal Analytical Intelligence Products

Information derived from national security letters may also be used in the development of a variety of written products that are shared with FBI personnel, distributed more broadly within the Department, shared with Joint Terrorism Task Forces, or disseminated to other members of the intelligence community.

However, FBI counterintelligence and counterterrorism personnel told us that FBI practice and policy discourage reference to the source of the information discussed in these products in order to protect the FBI's sources and methods. Nonetheless, field personnel we interviewed, including intelligence analysts and financial analysts, told us that the following types of analytical products frequently contain information derived from national security letters, particularly if they are based on information derived from FISA authorities (electronic surveillance, physical searches, or pen register/trap and trace devices). As noted above, one of the most important uses of national security letters is to develop evidence to support FISA applications. Since FISA applications for electronic surveillance must contain evidence



The following are examples of FBI analytical intelligence products that use information obtained from NSLs.

- **Intelligence Information Reports**

An Intelligence Information Report (IIR) contains "raw intelligence," which may include information from only one source or one area that has not been fully "vetted" or verified. Headquarters and field personnel told us that FBI analysts sometimes use raw data obtained from national security letters – such as telephone numbers or Internet e-mail account information – in preparing IIRs. For example, if the initial analysis of telephone toll records and subscriber information reveals important ties between a known terrorist and others, the analyst may generate an IIR quickly if the geographic location of the subject is known. In this circumstance, the IIR

States Attorneys' Offices (described below), the Drug Enforcement Administration, the Federal Bureau of Prisons, and other Department components, including components whose personnel serve on Joint Terrorism Task Forces, such as prosecutors and intelligence research specialists.

Joint Terrorism Task Forces: Joint Terrorism Task Forces (JTTFs) are composed of representatives of federal, state, and local law enforcement agencies who respond to leads, investigate, make arrests, provide security for special events, and collect and share intelligence related to terrorist threats.⁹⁴ Some task force members are designated Task Force Officers, some of whom obtain the necessary clearances to obtain access to FBI information, including information derived from national security letters and other investigative techniques. These Task Force Officers also are authorized to access information stored in FBI databases such as ACS, the specialized application for telephone data, and IDW which, as noted above, contain information derived from NSLs. Task Force Officers who obtain the required security clearances and sign access agreements are issued accounts to access these databases (with the exception of case information to which access was restricted due to special sensitivities). Consequently, Task Force Officers with approved user accounts are able to access databases that house raw data derived from NSLs. In addition, Task Force Officers have access to formal analytical products derived, at least in part, from national security letters and other information. However, Task Force Officers are not permitted to share this information with their host agencies unless specifically authorized in memoranda of understanding between the FBI and the host agency.

Other Federal Agencies: The Attorney General's NSI Guidelines authorize the FBI to share information obtained through intelligence activities conducted under the Guidelines with other federal law enforcement agencies and the Department of Homeland Security.⁹⁵ Since many federal agencies are represented on JTTFs, the JTTFs are a significant information-sharing mechanism for information derived from national security letters as well as other investigative techniques.⁹⁶ In addition, several FBI field divisions told us that they disseminated information

⁹⁴ Each of the FBI's 56 domestic field divisions contains at least one JTTF, and as of March 2005 the FBI operated JTTFs in 100 U.S. cities.

⁹⁵ NSI Guidelines, VII(B)(3).

⁹⁶ For example, members of the JTTF in a major FBI field division include representatives from the United States Attorney's Office, United States Marshals Service, United States Postal Service, United States Secret Service, Department of Homeland Security, Federal Protective Service, United States Coast Guard, Department of Defense, Central Intelligence Agency, as well as representatives from state and local law enforcement, including the state police and the city police department.

derived from NSLs to the Department of Energy and the Department of Commerce in connection with counterintelligence investigations.

During our site visits to four FBI field offices, we reviewed examples of documented dissemination of IIRs, Intelligence Bulletins, and Intelligence Assessments to other federal agencies. For example, case agents on counterintelligence squads disseminated NSL-derived information to the Commerce Department's Export Control Agency to identify products on an export control list. Case agents on counterterrorism squads disseminated NSL-derived information to the Immigration and Customs Enforcement branch in the Department of Homeland Security related to the investigation of potential immigration charges.

Members of the Intelligence Community: The NSI Guidelines authorize the FBI to share information covered by various memoranda of understanding with members of the intelligence community.⁹⁷ Consequently, FBI analytical products that contain information from national security letters are disseminated to other members of the intelligence community. FBI field offices told us that they disseminated information derived from national security letters to the Central Intelligence Agency, National Reconnaissance Office, Defense Intelligence Agency, Naval Criminal Investigative Service, Air Force Office of Special Investigations, and the National Security Agency. As noted above, these analytical products normally do not reference the source of the information used to produce the product.

Private Sector Entities: Together with threat information derived from other investigative tools, information from national security letters is included in threat advisories that are communicated to private sector entities. FBI officials in the four divisions we visited during the review told us that they brief members of the private sector on terrorist threats or other threats associated with special events, such as the Olympics or the World Series. These briefings may advise the security officials of private companies of the nature of the threat, but they do not communicate details of pending investigations or what investigative tools were used to identify and assess the severity of the threat.

Foreign Governments: The NSI Guidelines authorize the FBI to share information obtained through intelligence activities under the Guidelines, which include information from national security letters, with foreign authorities under specified circumstances when the dissemination is in the interest of the United States.⁹⁸ Information derived from national security letters can also generate leads that are passed on to foreign government counterparts.

⁹⁷ NSI Guidelines, VII(B)(3).

⁹⁸ NSI Guidelines, VII(B)(6).

The CAU is designated an “operational support unit” rather than an operational unit. The consequence of this status is that under FBI internal policy the CAU cannot initiate counterterrorism investigations under the NSI Guidelines and cannot issue national security letters. NSLB attorneys told us that to the extent the CAU wants to obtain telephone toll billing records or other records under the ECPA NSL statute, the CAU has two options. One, it can ask the Headquarters Counterterrorism Division or an appropriate field division counterterrorism squad to issue a national security letter from an existing investigation to which the request was relevant. In those instances, as described in Chapter Three, in order to meet the NSI Guidelines’ and ECPA standards, the CAU needs to generate approval memoranda articulating the relevance of the information sought to the pending investigation. Alternatively, if there is no pending investigation, the CAU can ask Headquarters operating units in the Counterterrorism Division or field office squads to: a) open a new counterterrorism investigation based on predication the CAU supplies that is sufficient to meet the NSI Guidelines and the ECPA, and b) issue a national security letter seeking information relevant to the new investigation.

As discussed in Chapter Three, only Special Agents in Charge of the FBI’s field offices and specially delegated senior Headquarters officials are authorized to issue national security letters.

1. FBI Contracts With Three Telephone Companies

Following the September 11 attacks, the FBI’s New York Division formed a group to assist in the analysis of telephone toll billing records that were needed for the criminal investigations of the 19 hijackers. A small group of agents and analysts assigned to examine the communication networks of the terrorists evolved into a domestic terrorism squad in the New York Division known as DT-6. During this time, the FBI’s New York Division developed close working relationships with private sector companies, including telephone companies that furnished points of contact to facilitate the FBI’s access to records held by these companies, including telephone records. The Supervisory Special Agent (SSA) who supervised DT-6 told us that he obtained Headquarters approval of and Headquarters financing for an arrangement whereby a telephone company representative would work with the New York Division to expedite the FBI’s access to the telephone company’s databases.

The SSA said that case agents on DT-6 generally provided grand jury subpoenas to the telephone company prior to obtaining telephone records. The grand jury subpoenas issued to the telephone company were signed by Assistant United States Attorneys who worked with FBI agents in the

criminal investigations growing out of the September 11 attacks.¹²⁴ However, in the period following the September 11 attacks, instead of initially sending a grand jury subpoena the case agents frequently furnished a “placeholder” to the telephone company in the form of a letter stating, in essence, that exigent circumstances supported the request. These “placeholder” letters – also referred to as “exigent letters” – were signed by SSAs or subordinate squad personnel.¹²⁵

Between late 2001 and the spring of 2002, the value of the FBI’s access to the telephone company prompted the FBI to enter into contracts with three telephone companies between May 2003 and March 2004. The requests for approval to obligate funds for each of these contracts referred to the Counterterrorism Division’s need to obtain telephone toll billing data from the communications industry as quickly as possible. The three memoranda stated that:

Previous methods of issuing subpoenas or National Security Letters (NSL) and having to wait weeks for their service, often via hard copy reports that had to be retyped into FBI databases, is insufficient to meet the FBI’s terrorism prevention mission.

The three memoranda also stated that the telephone companies would provide “near real-time servicing” of legal process, and that once legal process was served telephone records would be provided.

The CAU worked directly with telephone company representatives in connection with these contracts. Moreover, on the FBI’s Intranet web site, CAU referenced its capacity to facilitate the acquisition of telephone records pursuant to the contracts. CAU presentations to counterterrorism squads in several field divisions also described the unit’s capabilities, including its access to telephone company records. The slides used in CAU presentations referred to the CAU’s ability to “provide dedicated personnel to service subpoenas/NSLs 24 x 7.” In describing how the CAU should receive requests from the field, the slides noted that

Field office prepares NSL or FGJS for CAU to serve on appropriate telecom provider.

¹²⁴ The SSA told us that an attorney with the telephone company established a tracking system to ensure that grand jury subpoenas were issued to cover all of the records obtained from the telephone company employees. The SSA also said that he checked regularly with a point of contact at the telephone company to determine if the FBI had fallen behind in providing legal process for these records. The SSA said he was confident that grand jury subpoenas were issued to cover every request.

¹²⁵ The SSA said that DT-6 case agents would sometimes provide the placeholder letters to the telephone company to initiate the search for records. The SSA said that in most instances by the time the records were available, a grand jury subpoena was ready to be served for the records.

-- Once paper received, CAU will obtain tolls/call details.

Thus, from this presentation, it appears that the CAU contemplated that the FBI would serve national security letters or grand jury subpoenas prior to obtaining telephone toll billing records and subscriber information pursuant to the three contracts, in conformity with the ECPA NSL statute.¹²⁶

The Assistant Director of the Counterterrorism Division told us that based on numerous FBI briefings he received during his tenure, he directed his subordinates to contact the CXS Section Chief to ensure that the capabilities of the three companies were used. However, he also told us that he was unaware that any of the three companies were providing telephone toll billing records without first receiving duly authorized national security letters.

2. The Exigent Letters to Three Telephone Companies

The SSA who supervised DT-6 following the September 11 attacks told us that by late 2001 he and other DT-6 personnel were assigned to assist in the establishment of CAU at FBI Headquarters, and that they would have brought with them to Headquarters a copy of the exigent letter that had been used in the criminal investigations of the September 11 attacks to obtain information from the telephone company in New York. This letter was used by CAU personnel as a model to generate requests to the three telephone companies under contract with the FBI to provide telephone toll billing records or subscriber information. These exigent letters typically stated:

Due to exigent circumstances, it is requested that records for the attached list of telephone numbers be provided. Subpoenas requesting this information have been submitted to the U.S. Attorney's Office who will process and serve them formally to [information redacted] as expeditiously as possible.

In response to our request, the FBI provided the OIG copies of 739 exigent letters addressed to the three telephone companies dated between March 11, 2003, and December 16, 2005, all but 4 of which were signed. The signed exigent letters included 3 signed by CXS Assistant Section Chiefs, 12 signed by CAU Unit Chiefs, 711 signed by CAU Supervisory Special Agents, 3 signed by CAU special agents, 2 signed by intelligence analysts, 1 signed by an intelligence operations specialist, and 3 that

¹²⁶ NSLB attorneys told us that NSLB attorneys were not consulted about the three contracts with the telephone companies or the procedures and administrative steps that CAU took following their implementation to obtain telephone toll billing records pursuant to the contracts. The FBI-OGC attorneys and a former CAU Unit Chief told us that to their knowledge the only OGC lawyers involved in reviewing the contracts were procurement lawyers.

contained signature blocks with no titles. Together, the 739 exigent letters requested information on approximately 3,000 different telephone numbers. The three highest volume exigent letters sought telephone toll billing or subscriber information on 117, 125, and 171 different telephone numbers.

We determined that contrary to the provisions of the contracts and the assertions in CAU's briefings that the FBI would obtain telephone records only after it served NSLs or grand jury subpoenas, the FBI obtained telephone toll billing records and subscriber information prior to serving NSLs or grand jury subpoenas. Moreover, CAU officials told us that contrary to the assertion in the exigent letters, subpoenas requesting the information had not been provided to the U.S. Attorney's Office before the letters were sent to the telephone companies. Two CAU Unit Chiefs said they were confident that national security letters or grand jury subpoenas were ultimately issued to cover the FBI's receipt of information acquired in response to the exigent letters. The Unit Chiefs said that they relied on the telephone company representatives to maintain a log of the requests and to let CAU personnel know if any NSLs or grand jury subpoenas were needed. However, the Unit Chiefs acknowledged that because the CAU did not maintain a log to track whether national security letters or grand jury subpoenas were issued to cover the exigent letter requests and did not maintain signed copies of the exigent letters, they could not provide documentation to verify that national security letters or grand jury subpoenas were in fact issued to cover every exigent letter request.

Pursuant to administrative subpoenas, the OIG obtained from the three telephone companies copies of national security letters and grand jury subpoenas that the FBI served on the telephone companies in connection with FBI requests for telephone toll billing records or subscriber information from 2003 through 2005. The three telephone companies provided 474 national security letters and 458 grand jury subpoenas. However, CAU personnel told us that some of these NSLs and grand jury subpoenas were not related to the exigent letters and that CAU could not isolate which NSLs or grand jury subpoenas given to the OIG by the telephone companies were associated with the exigent letters. CAU officials told us that the only way the CAU could attempt to associate an exigent letter with a national security letter or grand jury subpoena was to query the ACS database system with the telephone numbers referenced in the exigent letters. Because the CAU officials stated that this would be a labor intensive exercise, we asked them to query ACS for the NSLs, grand jury subpoenas, or related documentation associated with 88 exigent letters that we randomly selected from the 739 exigent letters provided to us by the FBI.

The FBI provided the results of ACS queries for the first 25 of the 88 letters. To try to demonstrate that it issued either national security letters or grand jury subpoenas to cover the FBI's acquisition of the records obtained in response to the exigent letters, the FBI pointed to various

exigent letters. Therefore, because of this clear finding in the first 25 letters and the labor intensive nature of the exercise, we did not ask the FBI to complete the sample of 88 letters.

3. Absence of Investigative Authority for the Exigent Letters

As discussed in Chapter Three, the national security letter statutes, the Attorney General's NSI Guidelines, and internal FBI policy require that Special Agents in Charge of field divisions or specially delegated Headquarters officials certify that the information sought in the national security letter is relevant to an authorized investigation. Since passage of the Patriot Act, the information requested in certain national security letters does not need to relate to the subject of the FBI's investigation, but can relate to other individuals as long as the information requested is relevant to an authorized national security investigation.

A former CAU Unit Chief told us that many of the exigent letters were generated in connection with significant Headquarters-based investigations as well as investigations in which the FBI provided assistance to foreign counterparts, such as investigations of the July 2005 London bombings. In some instances, CAU personnel said that the requests directed to CAU were communicated by senior Headquarters officials who characterized the requests as urgent. However, when CAU personnel gave the exigent letters to the three telephone companies, they did not provide to their supervisors any documentation demonstrating that the requests were related to pending FBI investigations, and many exigent letters were not sent in exigent circumstances. As described in Chapter Three, these are required elements for NSL approval documentation necessary to establish compliance with the ECPA NSL statute, the NSI Guidelines, and internal FBI policy. Moreover, we learned from interviews of CAU personnel and FBI documents that when CAU requested telephone records from the three telephone companies pursuant to exigent letters, there sometimes were no open or pending national security investigations tied to the request.

We found that in the absence of a pending investigation CAU sent leads either to the Headquarters Counterterrorism Division (ITOS-1 or ITOS-2) or to field offices asking them to initiate new investigations from which the after-the-fact NSLs could be issued. However, CAU personnel told us that the Counterterrorism Division units and field personnel often resisted generating the documentation for these new investigations or declined to act on the leads, primarily for three reasons. First, CAU often did not provide the operating units with sufficient information to justify the initiation of an investigation. Second, on some occasions, the documentation CAU supplied to the field divisions did not disclose that the

FBI had already obtained the information from the telephone companies.¹²⁹ When the field offices learned that the records had already been received, they complained to NSLB attorneys that this did not seem appropriate. Third, since Headquarters and field divisions were unfamiliar with the reasons underlying the requests, they believed that the CAU leads should receive lower priority than their ongoing investigations.

We concluded that, as a consequence of the CAU's use of the exigent letters to acquire telephone toll billing records and subscriber information from the three telephone companies without first issuing NSLs, CAU personnel circumvented the ECPA NSL statute and violated the NSI Guidelines and internal FBI policies. These matters were compounded by the fact that CAU used exigent letters in non-emergency circumstances, failed to ensure that there were duly authorized investigations to which the request could be tied, and failed to ensure that NSLs were issued promptly after the fact pursuant to existing or new counterterrorism investigations.

4. Efforts by the FBI's National Security Law Branch to Conform CAU's Practices to the Electronic Communications Privacy Act

NSLB attorneys responsible for providing guidance on the FBI's use of national security letter authorities told us that they were not aware of the CAU's practice of using exigent letters until late 2004. When an NSLB Assistant General Counsel learned of the practice at that time, she believed that the practice did not comply with the ECPA national security letter statute. Our review of contemporaneous e-mail communications and our interviews of CAU and NSLB personnel found that for nearly 2 years, beginning in late 2004, NSLB attorneys counseled CAU officials to take a variety of actions, including: discontinue use of exigent letters except in true emergencies; obtain more details to be able to justify associating the information with an existing national security investigation or to request the initiation of a new investigation; issue duly authorized national security letters promptly after the records were provided in response to the exigent letters; modify the letters to reference national security letters rather than grand jury subpoenas; and consider opening "umbrella" investigations out of which national security letters could be issued in the absence of another pending investigation.¹³⁰ In addition, NSLB offered to dedicate personnel to

¹²⁹ Similarly, when CAU on occasion asked the NSLB Deputy General Counsel to issue national security letters to cover information already obtained from the telephone companies in response to the exigent letters, CAU sometimes did not disclose in the approval documentation that the records already had been provided in response to the exigent letters. An NSLB Assistant General Counsel complained to CAU personnel about these omissions in December 2004.

¹³⁰ The Assistant General Counsel at first proposed the establishment of six "generic" or "umbrella" investigations files representing the recurring types of threats

CHAPTER SEVEN

OTHER NOTEWORTHY FACTS AND CIRCUMSTANCES RELATED TO THE FBI'S USE OF NATIONAL SECURITY LETTERS

As directed by the Patriot Reauthorization Act, in this chapter our report includes other “noteworthy facts and circumstances” related to the FBI’s use of national security letters that we found during our review. These matters include the interpretation of the Attorney General Guidelines’ requirement to use the “least intrusive collection techniques feasible” with regard to the use of national security letters; uncertainty about the types of telephone toll billing records the FBI may obtain pursuant to an Electronic Communications Privacy Act (ECPA) national security letter; the review by Division Counsel of NSL requests; the issuance of NSLs from control files rather than investigative files, in violation of FBI policy; the FBI’s use of “certificate letters” rather than Right to Financial Privacy Act (RFPA) national security letters to obtain records from Federal Reserve Banks; and the FBI’s failure to include in its NSL tracking database the use of NSLs to obtain information about individuals who are not subjects of FBI investigations.

I. Using the “least intrusive collection techniques feasible”

When FBI agents evaluate the investigative techniques available to them at different stages of FBI investigations – including the use of national security letters – one of the factors they must consider is the intrusiveness of the technique. According to the Attorney General’s Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines), the intrusiveness of the investigative technique must be compared to the seriousness of the threat to national security that is being investigated and the strength of the information indicating such a threat. The NSI Guidelines, which were in effect for all but the first ten months of this review and remain in effect today, state:

Choice of Methods. The conduct of investigations and other activities authorized by these Guidelines may present choices between the use of information collection methods that are more or less intrusive, considering such factors as the effect on the privacy of individuals and potential damage to reputation. As Executive Order 12333 § 2.4 provides, “the least intrusive collection techniques feasible” are to be used in such situations. The FBI shall not hesitate to use any lawful techniques consistent with these Guidelines, even if intrusive, where the degree of intrusiveness is warranted in light of the seriousness of a threat to the national security or the strength of the

information indicating its existence. This point is to be particularly observed in investigations relating to terrorism.¹⁴⁴

However, during our review, we found that no clear guidance was given to FBI agents on how to reconcile the limitations expressed in the Attorney General Guidelines, which reflect concerns about the impact on privacy of FBI collection techniques, with the expansive authorities in the NSL statutes.¹⁴⁵

For example, during our review, several senior FBI attorneys told us that legal precedents suggest that NSLs seeking telephone toll billing records and subscriber information do not implicate privacy interests under the Fourth Amendment. Several also said that they consider NSLs seeking financial records and consumer full credit reports to be more intrusive than NSLs seeking telephone toll billing records or subscriber information. However, the national security letter statutes and internal FBI policies do not address which of the national security letter authorities are more intrusive than others or the relative intrusiveness of NSLs compared to other investigative techniques.

These issues raise difficult questions that regularly arise regarding the FBI's use of national security letters. For example, under the NSI Guidelines, should case agents access NSL information about parties two or three steps removed from their subjects without determining if these contacts reveal suspicious connections? In light of the "least intrusive collection techniques feasible" proviso in the Attorney General Guidelines, is there an evidentiary threshold beyond "relevance to an authorized investigation" that should be considered before financial records or full credit histories are obtained on persons who are not investigative subjects? Are NSLs more or less intrusive than other investigative techniques authorized for use during national security investigations, such as physical surveillance? Yet, if agents are hindered from using all types of NSLs at early stages of investigations, this may compromise the FBI's ability to pursue critical investigations of terrorism or espionage threats or to reach resolution expeditiously that certain subjects do not pose threats.

The FBI Headquarters and field personnel we interviewed said that there is no uniform answer to the difficult question of how to use and sequence NSLs. Instead, they said that individualized decisions are made based on the evidence developed as the investigation proceeds. The FBI

¹⁴⁴ NSI Guidelines, § I(B)(2).

¹⁴⁵ OGC sent guidance on November 28, 2001, that referred to the "least intrusive" means proviso contained in the applicable FCI Guidelines. The guidance stated that supervisors should keep [the proviso] in mind when deciding whether or not a particular use of NSL authority is appropriate. The greater availability of NSLs does not mean that they should be used in every case.

General Counsel also expressed this view, stating that she believes that the use and sequencing of national security letters is best left to the experienced judgment of field supervisors. However, several Division Counsel told us that they believe it would be helpful if FBI-OGC's National Security Law Branch (NSLB) provided guidance on the interrelationship between the Attorney General's NSI Guidelines and the NSL statutes.

The impact of the FBI's investigative choices when using national security letters is magnified by three factors. First, as discussed in Chapter Four, the FBI generates tens of thousands of NSLs per year on the authority of Special Agents in Charge, and the predication standard – relevance to an authorized investigation – can easily be satisfied. Second, we found that FBI Division Counsel in field offices have asked NSLB attorneys in FBI Headquarters for ad hoc guidance on application of the “least intrusive collection techniques feasible” proviso, suggesting a need for more clarity or at least a frame of reference.¹⁴⁶ Third, neither the Attorney General's NSI Guidelines nor internal FBI policies require the purging of information derived from NSLs in FBI databases, regardless of the outcome of the investigation. Thus, once information is obtained in response to a national security letter, it is indefinitely retained and retrievable by the many authorized personnel who have access to various FBI databases.

We recognize that there cannot be one model regarding the use of NSLs in all types of national security investigations, and that the FBI cannot issue definitive guidance addressing when and what types of NSLs should issue at each stage of investigations. The judgment of FBI agents and their supervisors, coupled with review by Chief Division Counsel and Special Agents in Charge or senior Headquarters officials, are critical to ensuring the appropriate use of these NSLs and preventing overreaching. However, we believe that the meaning and application of the Attorney General Guidelines' proviso calling for use of the “least intrusive collection techniques feasible” to the FBI's use of national security letter authorities should be addressed in general FBI guidance as well as in the training of special agents, Chief Division Counsel, and all FBI officials authorized to sign NSLs.¹⁴⁷ With the FBI's increasing reliance on national security letters

¹⁴⁶ For example, the need for guidance was raised by a CDC in the context of considering whether it is appropriate to issue financial record and consumer full credit report NSLs in every terrorism investigation.

¹⁴⁷ One senior NSLB attorney told us that he does not believe that the training given to Special Agents in Charge adequately focuses on the use of NSL authorities, particularly in light of the volume of NSLs that field divisions are issuing. This attorney and other FBI Headquarters personnel told us that when NSLs are addressed at SAC training conferences, the focus is on the statutory requirements and internal FBI policies, such as the fact that SACs may not delegate authority to sign NSLs to Acting Special Agents in Charge or others.