and inaccurate letters over a 3-and-a-half-year period is both surprising and troubling.

Moreover, not only did the FBI issue exigent letters to obtain records from the three on-site communications service providers, the FBI used even less formal means to request or obtain telephone toll billing records or other information. We found that the FBI obtained records or information from each of the on-site communications service providers in response to e-mail, face-to-face requests, requests on pieces of paper (including post-it notes), and telephonic requests without first providing legal process or even exigent letters. These informal requests were made in connection with major operations as well as other international terrorism, domestic terrorism, and criminal investigations. As described in Chapter Six, like exigent letters, these other types of informal requests did not constitute legal process under the ECPA and FBI policy.

We noted in our first NSL report that FBI personnel were required by FBI policy to document information demonstrating the FBI's authority to use NSLs in national security investigations. The predication for an NSL request was supposed to be documented in NSL approval memoranda, known as approval ECs. These approval ECs, which were routinely uploaded into the FBI's Automated Case Support System, identified the underlying national security investigation, summarized the facts establishing the predication for the requests, and described the relevance of the information requested to the investigation.[78] The steps required to complete these approval ECs and the chain of command required to approve each NSL request were designed to ensure that the FBI satisfied statutory and Attorney General Guidelines' requirements for using NSLs.

In contrast, when CAU personnel issued exigent letters or made other types of informal requests for records and information from the on-site providers, they did not document the authority for their requests or explain the investigative reasons why the records were needed. The exigent letter requests also were not subject to any supervisory or legal review. Specifically, exigent letters and other informal requests were *not*: (1) accompanied by approval ECs documenting the predication for the requests, specifying the date range of the records requested, and certifying the relevance of the information sought to pending national security investigations; (2) reviewed and approved by FBI attorneys; (3) approved by FBI supervisors; or (4) signed by one of the limited number of senior FBI

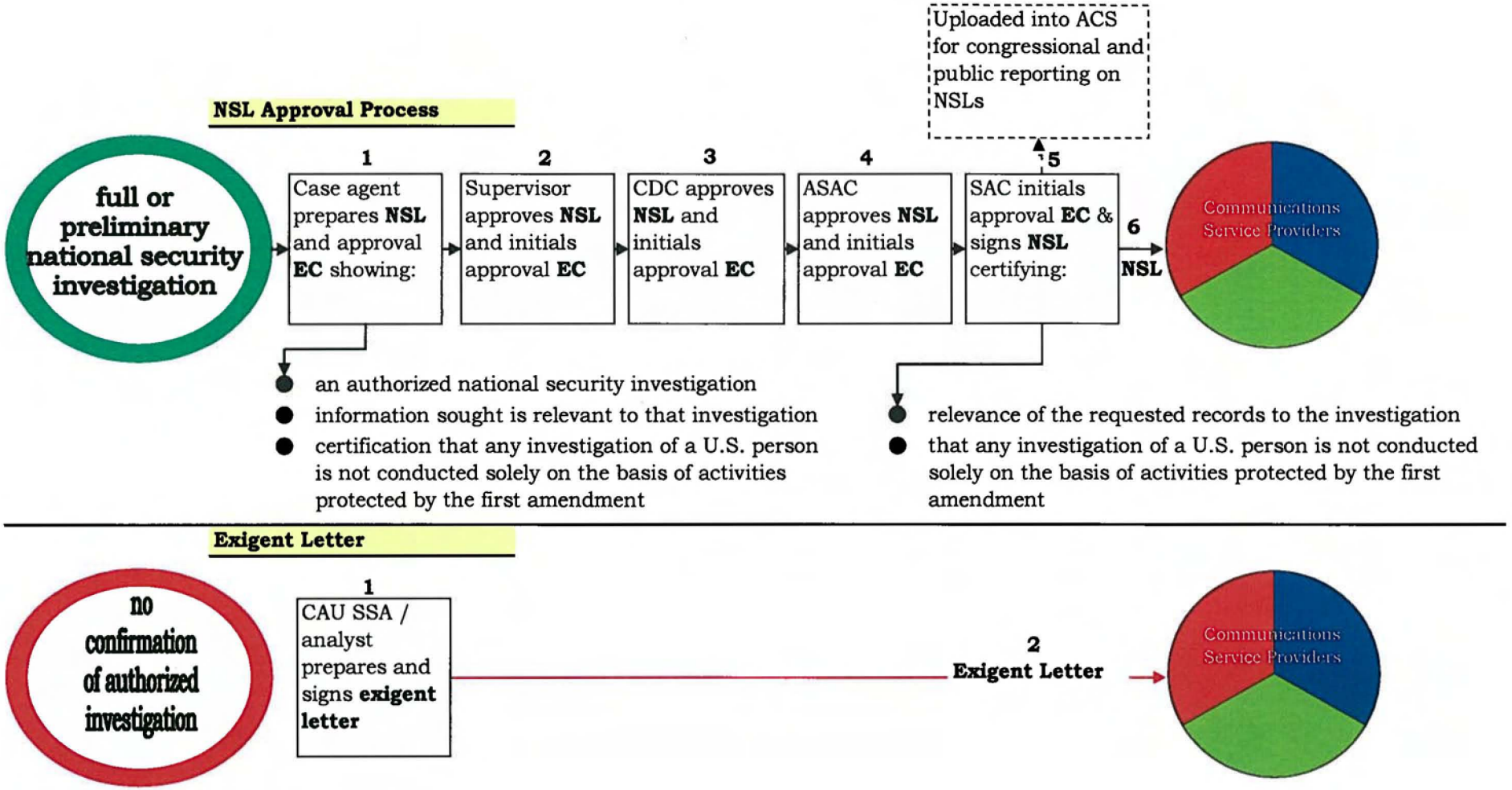
---

[78] OIG, NSL I, 23-25.

personnel authorized to sign NSLs.[79] Similarly, the exigent letters did not meet the legal requirements in the Patriot Act and Patriot Reauthorization Act that senior FBI officials certify in writing the relevance of the records sought to authorized national security investigations and that any investigations of U.S. persons are not based solely on activities protected by the First Amendment. We illustrate in Diagram 2.2 (next page) the differences between the 4-step approval process required for issuing NSLs and the 1-step process used by CAU personnel to issue exigent letters to obtain the same information:

[79] Prior to June 1, 2007, a legal review and approval by an FBI attorney was not required. However, guidance issued by the FBI OGC in November 2001 recommended such a review. Office of the General Counsel, Federal Bureau of Investigation, electronic communication to All Field Offices, Counterterrorism, and National Security, November 28, 2001.

DIAGRAM 2.2
Comparison of NSL Approval Process with Exigent Letters



In fact, the procedure for preparing and issuing exigent letters was so lax that employees of the on-site providers told us that they frequently prepared the exigent letters themselves. Indeed, a Company A analyst told us that to facilitate his preparation of exigent letters he created an icon on his computer desktop so he could easily retrieve and generate the form letter. We believe this is an egregious breakdown in the responsibility assigned to the FBI to obtain ECPA-protected records, and it further illustrates the lack of appropriate controls by the FBI on this important and intrusive investigative tool.

Another result of the abbreviated, unsupervised procedures for issuing exigent letters and other types of informal requests was that FBI requesters did not document whether there was an open national security investigation to which the request was relevant – a key certification required to issue an NSL for toll billing records or subscriber information under Section 2709 of the ECPA. Indeed, as the FBI's analysis of whether it will retain records acquired through exigent letters and other informal requests has shown (which we describe in Chapter Four of this report), the FBI has concluded that records for hundreds of telephone numbers must be purged from FBI databases because there was no open national security investigation at the time of the request and no open national security investigation to which the request could be tied when the retention issue was analyzed years later.

Also troubling was that most of the exigent letters and other informal requests did not include date ranges for the records requested. Of the 722 exigent letters signed by CAU personnel from 2003 through 2006, only 77 (11 percent) specified a date range for the records requested. Similarly, the CAU's other informal requests to the on-site communications service providers (such as those communicated by e-mail, in person, on pieces of paper, or by telephone) frequently did not have date parameters. As further described in Chapter Four of this report, the absence of date restrictions in many exigent letters and other types of informal requests had significant consequences. First, it meant that the FBI often obtained substantially more telephone records, covering longer periods of time, than FBI agents typically obtain when serving NSLs with date restrictions. Second, in cases where the date range established the relevance of the information sought to the investigation, its omission violated the ECPA's relevance requirement.[80]

---

[80] The ECPA NSL statute requires a certification that "the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities . . . ." See 18 U.S.C. § 2709(b)(1). Similarly, the emergency voluntary disclosure provision requires, since March 2006, that the information disclosed be "relat[ed] to the emergency." 18 U.S.C. § 2702(c)(4).

Moreover, by not reviewing records obtained in response to exigent letters and other types of informal requests, CAU personnel compounded problems arising from the lax procedures at the front end of these requests. CAU personnel told us, and documents we reviewed confirmed, that records obtained in response to exigent letters and other informal requests were routinely uploaded into a [redacted] database when received from the on-site communications service providers. However, this uploading normally occurred without verification that the records obtained matched the requests. Further, the original FBI requesters often did not have access to this database or know that CAU personnel were uploading records into the database.

We found in our first NSL review that the FBI did not always examine records obtained in response to NSLs prior to uploading the records into FBI databases.[81] However, in those instances where the communications service providers responded to routine NSLs issued by FBI field offices, the case agents or Intelligence Analysts who had initiated these requests would sometimes review the records before they were uploaded into FBI databases. Because of their familiarity with the underlying investigations, these case agents or Intelligence Analysts could identify records the FBI did not request, or had requested by mistake, and take corrective action before the records were uploaded or placed in investigative case files.

In contrast, CAU personnel routinely uploaded records obtained in response to exigent letters and other informal processes into the [redacted] database upon receipt, without any review. The CAU SSAs and Intelligence Analysts said they were for the most part unaware of the facts of the investigations and were acting merely as conduits between the requesters and the on-site communications services providers. Indeed, CAU personnel did not even retain copies of the exigent letters or documentation of the other types of informal requests and therefore were unable to confirm that they received responsive records. This meant that neither CAU personnel nor anyone else in the FBI determined whether the FBI had received unauthorized

---

[81] FBI personnel were not required until June 1, 2007, after the OIG's first NSL report was issued, to confirm that records obtained in response to NSLs matched the requests in the NSLs before uploading them into FBI databases. We found in our first and second NSL reports that the FBI obtained unauthorized collections in response to many NSLs, findings confirmed by the FBI's review of a statistical sample of NSLs issued from 2003 through 2006. The unauthorized collections included records not requested in the NSLs. See OIG, NSL I, 73-84; OIG, NSL II, 26-28, 82-99.

collections, handled the overcollected materials appropriately, and made required reports to the President's Intelligence Oversight Board (IOB).[82]

B. "Sneak Peeks"

We also identified the FBI's practice of obtaining "sneak peeks" for telephone toll records in the providers' databases, a practice that we concluded violated the ECPA statute (18 U.S.C. § 2702(a)(3)). There is no provision in the ECPA allowing the FBI to obtain information about these records without either issuing legal process or making requests for voluntary disclosure in qualifying emergencies, pursuant to 18 U.S.C. § 2702(c)(4).

Because CAU personnel failed to keep records of sneak peek requests, we were unable to determine how often such requests were made during the period covered by our review, whether the requests were pertinent to FBI investigations, in what circumstances they were made, and what, if anything, the providers were told about the reasons for these requests. However, we found that these requests were routine. One Company A analyst told us he responded to these requests on a daily basis, a Company C employee told us that these requests were approximately one-half of the requests he received from the CAU, and a Company B employee told us that he responded to these requests up to three times per week. The on-site Company C employee's log and e-mails of the employees of all three on-site providers also demonstrate that such requests were routine.

Although CAU Unit Chief Rogers was aware of and approved sneak peek requests, we found that he issued no guidance and failed to require supervisory review or establish internal controls regarding their use. Rogers said he understood sneak peeks to be requests to see if the providers "even had

---

[82] Executive Order 12863, which has since been modified, requires the Department to report intelligence violations to the President's Intelligence Oversight Board. According to Executive Order 12863, possible intelligence violations include any activities that "may be unlawful or contrary to Executive Order or Presidential Directive."

"Unauthorized collections" is a phrase used to describe several circumstances in which the FBI receives information in response to NSLs that was not requested or was mistakenly requested. For example, many unauthorized collections occur due to errors on the part of NSL recipients when they provide more information than was requested (such as records for a longer period of time or records on additional persons). The FBI refers to these matters as "over collections" or "overproductions." We refer to these as "initial third party errors" because, while the NSL recipient may initially have provided more information than requested, the FBI may or may not have compounded the initial error by using or uploading the information. Other unauthorized collections can result from FBI errors, such as when a typographical error in the telephone number or e-mail address results in the acquisition of data on the wrong person. See NSL II at 141.

data at all" and whether it was worthwhile pursuing an NSL. Youssef said he had no "first-hand knowledge" that CAU personnel requested sneak peeks from the on-site providers and did "not know for a specific fact . . . that it actually happened." However, Youssef added that "maybe someone [in the CAU] has used it."

We found that FBI supervisors in the CTD's chain of command, above the CAU Unit Chief, either did not know about the practice, did not have an accurate understanding of the practice, or did not understand the legal implications of providing responsive information without legal process. For example, former CXS Assistant Section Chief John Chaddic believed, incorrectly, that in response to sneak peek requests, the providers only informed the FBI whether the number was or was not a valid telephone number, but no further details. Former CTD Deputy Assistant Director John Lewis said it was his understanding that the FBI could use sneak peeks to "get records that would be of interest to us" without legal process, stating, "it's also why I think the phone company was there."

On August 28, 2007, the FBI OGC requested a legal opinion from the Department's Office of Legal Counsel (OLC) regarding three questions relating to the FBI's authority under the ECPA, including sneak peeks. One question stated that, "on occasion, FBI employees may orally ask an electronic communications provider if it has records regarding a particular facility (e.g., a telephone number) or person." The request asked whether under the ECPA the FBI can lawfully "obtain information regarding the existence of an account in connection with a given phone number or person," by asking a communications service provider, "'Do you provide service to 555-555-5555?' or 'Is John Doe your subscriber?'"

However, based on information we developed in our investigation, we determined that the hypothetical example used by the FBI OGC in the question it posed to the OLC did not accurately describe the type of information the FBI often obtained in response to sneak peek requests. As described above the FBI sometimes obtained more detailed information about calling activity by target numbers, such as whether the telephone number belonged to a particular subscriber, the number of calls to and from the telephone number within certain date parameters, the area codes [redacted] called, and call duration.

On November 5, 2008, the OLC issued its legal opinion on the three questions posed by the FBI. In evaluating if a provider could tell the FBI consistent with the ECPA "whether a provider serves a particular subscriber or

a particular telephone number," the OLC concluded that the ECPA "bars providers from complying with such requests."[83] In reaching its conclusion, the OLC opined that the "phrase 'record or other information pertaining to a subscriber' [in 18 U.S.C. § 2702(a)(3)] is broad" and that since the "information [requested by the FBI] is associated with a particular subscriber, even if that subscriber's name is unknown" it cannot be disclosed under the ECPA unless the disclosure falls within one of the ECPA exceptions.

As described in Chapter Two, the information the on-site providers gave to CAU personnel in response to their sneak peek requests often included more detailed information about the subscribers or customers than simply whether the provider had records regarding particular telephone numbers or persons. Therefore, we concluded that this information also was information "associated with a particular subscriber" within the meaning of 18 U.S.C. § 2702(a)(3).

As described above, the ECPA prohibits the disclosure to the government of toll records or information related to a subscriber except in certain limited circumstances set forth in the statute. The relevant exceptions require providers to disclose such information in response to compulsory legal process, such as national security letters, and also permit voluntary disclosures based upon the providers' good faith belief of a qualifying emergency.[84] We found that the FBI did not serve legal process under the ECPA for the information it received pursuant to sneak peeks.

In addition, we do not believe that the FBI's sneak peek practice complied with the ECPA's emergency voluntary disclosure provision for several reasons. First, the practice was described to us as a routine occurrence in the CAU, not limited to "exigent" circumstances. Second, some of the specific instances where the sneak peek practice was used included media leak and fugitive investigations, which clearly did not meet the emergency voluntary disclosure provision. Third, the FBI's lack of internal controls over the sneak peek practice made it impossible for us – or the FBI – to reliably determine how many or in what circumstances sneak peek requests were made, and what the providers were told or believed about the reasons for these requests. Therefore,

---

[83] The OLC identified a very narrow exception under 18 U.S.C. § 2702(a)(3) for disclosure of whether a particular telephone number was among those assigned or belonging to the provider but not "whether the provider has given [the number] to a subscriber."

[84] As described previously, prior to March 2006, this exception required the provider to have a "reasonable belief" that a qualifying emergency existed.

we found that the FBI's sneak peek practice violated the ECPA in many cases.[85]

C. Calling Circle/Community of Interest [redacted]

In addition, we believe that the community of interest [redacted] practices used by the FBI were improper.

First, the FBI's lack of documentation made it difficult to determine under what circumstances and how often community of interest [redacted] were conducted. We identified 52 exigent letters and over 250 NSLs and 350 grand jury subpoenas containing requests for community of interest [redacted] However, we could not determine whether Company A in fact [redacted] such [redacted] in response to all these requests and, if so, whether the [redacted] were limited on an ad hoc basis, for example, [redacted] Nor could we determine how often records or information about the telephone numbers other than the numbers listed in the legal process or exigent letters were provided to the FBI. Similarly, while Company A records show that from 2004 through 2007 the on-site Company A analysts used the Company A community of interest [redacted] to review records for 10,070 [redacted] telephone numbers, Company A could not distinguish whether these numbers were [redacted] as part of Company A's [redacted] service or in response to FBI requests. Company A also could not tell us whether these [redacted] records were actually provided to the FBI.[86]

Second, when FBI personnel issued NSLs that included requests for community of interest [redacted], they did not consistently assess the relevance of the [redacted] numbers before making the request. Instead, community of interest requests were often included in the boilerplate attachments to NSLs. The FBI issued NSLs that requested community of interest [redacted] without conducting, or documenting in the approval ECs, any

---

[85] In a draft of this report given to the FBI in April 2009, the OIG recommended that the FBI issue guidance specifically prohibiting the use of sneak peeks. In June 2009, the FBI posted guidance on its Corporate Policy Intranet prohibiting sneak peek practices. The guidance referred to the OLC legal opinion and also stated that FBI employees "may not informally seek statutorily protected information prior to the issuance of process." The FBI told us that this guidance will be incorporated into the next revision of its Domestic Investigations and Operations Guide.

[86] As noted above, we believe that most of Company A's community of interest [redacted] without requests from the FBI as part of Company A's [redacted] service, and records were not provided to the FBI. (S//NF)

assessment of the possible relevance of [redacted] telephone numbers to the underlying investigation. Absent such an assessment, we believe the FBI did not satisfy the ECPA requirement to issue NSLs in national security investigations only upon certification by those authorized to sign NSLs that the records are relevant to authorized national security investigations.[87] Moreover, although we identified instances in which some community of interest [redacted] requests were limited to telephone numbers with [redacted] or from [redacted], we do not believe these limitations necessarily satisfied the ECPA certification requirement or corresponding provisions of the Attorney General's NSI Guidelines and FBI policy.[88]

Third, FBI personnel who made the decisions to request community of interest [redacted] after reviewing [redacted] records were not among the officials to whom the FBI Director delegated authority under the ECPA to sign NSLs. CAU Intelligence Analysts and SSAs are subordinate to the FBI officials who are authorized to sign NSLs. Yet, after reviewing the [redacted] records, these subordinate FBI employees sometimes asked the on-site Company A analysts to provide [redacted] records. We believe that if the signers of the NSLs did not themselves determine that the [redacted] records were relevant to an authorized counterterrorism investigation, the [redacted] of the [redacted] records would violate the ECPA, even if the community of interest request was included in the NSL attachment.

Fourth, when the FBI received digital records from Company A in response to its community of interest [redacted] requests, the records did not identify or otherwise distinguish toll billing records [redacted] in legal process or exigent letters. Moreover, the FBI uploaded responsive records into a [redacted] database, and the FBI did not separate records on the target numbers listed in legal process from the records [redacted] and provided in response to community of interest [redacted] requests. It is therefore likely that the records of thousands of calls to and from [redacted] telephone numbers were uploaded into the [redacted] database without the required relevance assessment by an authorized FBI official. Without additional research on these telephone

---

[87] See 18 U.S.C. § 2709(b).

[88] Limiting a community of interest [redacted] request to calls to or from [redacted] numbers by itself is not necessarily a relevance assessment. Similarly, limiting community of interest [redacted] requests to the [redacted] calls from a [redacted] would not necessarily satisfy the ECPA relevancy requirement.

numbers, the FBI is unable to identify which records are associated with [redacted] numbers and whether those numbers were relevant to the underlying investigations for which they were requested.

Fifth, when Company A [redacted] its community of interest [redacted] to review [redacted] telephone numbers as part of its [redacted] services in the absence of specific [redacted] requests from the FBI, the on-site Company A analysts sometime provided to the FBI information pertaining to a subscriber or a customer of its service. This also appears to violate the ECPA statute, which prohibits communications service providers from divulging "a record or other information pertaining to a subscriber to or customer of such service . . . to any governmental entity." See 18 U.S.C. § 2702(a)(3).

Finally, FBI e-mails indicate that in late 2004 FBI OGC attorneys became aware of but did not object to community of interest [redacted] requests for [redacted] telephone numbers. In May 2006, these attorneys also approved use of a boilerplate attachment for NSLs served on the on-site providers. This attachment listed community of interest records and 17 other types of information that "may be considered by [the providers] to be toll billing records." Although FBI General Counsel Caproni and NSLB Deputy General Counsel Thomas concluded that community of interest [redacted] requests for [redacted] telephone numbers could satisfy the ECPA relevance standard such that the FBI would not have to issue separate NSLs for the [redacted] records, the FBI did not issue written guidance on when such requests were appropriate. In March 2007, on the advice of the FBI OGC, the CTD directed that such requests [redacted]

In November 2007, the FBI OGC and the CTD generated draft guidance that incorporates the principle that the [redacted] Although this guidance has not yet been finalized, current FBI policy as stated in the Domestic Investigations and Operations Guide (DIOG) requires that the NSLB Deputy General Counsel approve community of interest requests and that [redacted] telephone numbers for which information has been obtained be reported to NSLB for congressional reporting purposes. In addition, the DIOG requires that the NSL approval EC demonstrate the relevance of [redacted] information to the national security investigation.

We agree with the principles articulated in the November 2007 draft guidance and the DIOG, [redacted] We concluded that in order to satisfy the requirements of the ECPA, relevance must be determined before the request is made.[89] We also agree that senior FBI officials and a Department attorney should approve such requests and that the record of telephone numbers [redacted] pursuant to these requests should be created for purposes of congressional reporting on NSL usage by the Department. However, CTD's guidance still has not been issued.

In sum, we concluded that the FBI's community of interest [redacted] practices were inappropriate and likely resulted in the FBI obtaining and uploading into a [redacted] database thousands of telephone records for [redacted] telephone numbers without the required certifications of relevance to an authorized international terrorism investigation by an authorized FBI official. In addition, we found that the FBI is unable to identify with certainty today which records in the database are associated with [redacted] numbers and whether those numbers were relevant to the underlying investigations for which they were requested. We also concluded that the FBI failed to review the implications of Company A's community of interest [redacted] capability when Company A first posted its analysts on-site at the CAU; failed to issue written guidance in coordination with the FBI OGC about the circumstances in which such requests were appropriate under the ECPA; failed to establish an approval process for such requests or ensure that the predication for these requests was properly documented in approval ECs; and failed to ensure that records sought in community of interest [redacted] requests were included in required reports to Congress on NSL usage.

---

[89] After reviewing a draft of this report, the FBI identified for us another draft policy, dated February 2008, that did not require approval by a Department attorney. We believe that the approach in the November 2007 draft guidance is superior. No final guidance has yet been issued by the FBI.

CHAPTER THREE
ADDITIONAL USES OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS

We found other irregularities in the way the FBI obtained telephone records and used the on-site communications services providers located in the Counterterrorism Division's (CTD) Communications Analysis Unit (CAU). As described in this chapter, we determined that the FBI obtained calling activity information from Company A and Company C on pre-determined "hot numbers" without legal process. In addition, in three media leak investigations, the FBI requested [redacted] and in two instances obtained reporters' toll billing records or calling activity information without prior approval by the Attorney General, in violation of federal regulation and Department policy.

We also determined that FBI Supervisory Special Agents (SSA) made inaccurate statements to the Foreign Intelligence Surveillance Court (FISA Court) in characterizing the source of records that the Department of Justice relied upon to support applications for electronic surveillance or pen register and trap and trace orders. In addition, an SSA assigned to the CAU signed administrative subpoenas to cover the FBI's earlier acquisition of telephone toll billing records through exigent letters or other informal requests in violation of the ECPA and the statute authorizing the use of administrative subpoenas in narcotics investigations (21 U.S.C. § 876). This CAU SSA and an SSA assigned to the FBI's [redacted] Field Division together signed 5 administrative subpoenas for telephone records that were dated from 7 to 44 days after the FBI had obtained the records without legal process, in violation of the ECPA.[90]

I. Obtaining Calling Activity Information on "Hot Numbers"

From 2004 through 2006 the FBI used a service offered by Company A and Company C referred to as "hot number [redacted]." When using this service, the FBI asked Company A or Company C to provide calling activity information for telephone numbers that CAU or other FBI personnel had identified as "hot numbers." As described below, the FBI sometimes included specific parameters in its requests – such as whether there were calls to or from a particular area code [redacted] After the [redacted] were set on the hot numbers, and without receiving court orders or any type of legal process

---

[90] As described below, some of these problems occurred in combination with the use of exigent letters or other informal requests.

authorizing release of this information, the on-site Company A and Company C employees informed CAU personnel when the hot numbers [redacted] In addition, the providers sometimes gave the FBI more information than just the fact that calling activity existed, such as call originating and terminating information. Based on records we examined from Company A, Company C, and the [redacted], we determined that the FBI requested calling activity information on at least 152 telephone numbers and obtained calling activity information for at least 42 hot numbers from 2004 through 2006.[91]

A. Legal Authority for Obtaining Calling Activity Information

The *Stored Communications Act*, 18 U.S.C. § 2701 *et.seq.*, a subtitle of the ECPA which includes the ECPA NSL statute, authorizes the FBI to obtain historical, stored data from communications service providers. However, the case law is unsettled whether legal process issued under the *Stored Communications Act* can also be used prospectively to obtain records that come into existence after the issuance of the legal process.[92]

---

[91] As described below, Company A told us that 87 telephone numbers were placed on a "hot" list by Company A for the FBI, but only 42 telephone numbers [redacted] We found documentation indicating that Company C placed at least 65 telephone numbers on a list for [redacted] and we found evidence that at least some of these numbers [redacted]

[92] This issue has arisen in the context of government requests to obtain prospective cell site location information. Courts are divided on whether the government can obtain such information through legal process issued pursuant to the *Stored Communications Act* (and the *Pen Register Act*), or whether the government must obtain a warrant based on probable cause. See, e.g., *In the Matter of the Application*, 534 F. Supp. 2d 585, 599-600 (W.D. Pa. 2008)(W.D. Pennsylvania decision), *aff'd*, 2008 WL 4191511 (W.D. Pa. 2008). Several cases denying the government's requests for prospective cell cite location information pursuant to the *Stored Communications Act* rely in part on the fact that the Act does not authorize collections of prospective information. See, e.g., *In re U.S. for Orders Authorizing Installation and Use of Pen Registers and Caller Identification Devices on Telephone Numbers*, 416 F. Supp. 2d 390, 395 (D. Md. 2006); *In re Application of the U.S. for an Order (1) Authorizing the Use of Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information*, 396 F. Supp. 2d 294, 311-14 (E.D.N.Y. 2005); *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 760-62 (S.D. Tex. 2005). But see, *In re: Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone*, 460 F.Supp2d 448, 452-459 (S.D.N.Y. 2006)(holding that the *Stored Communications Act* contains no explicit limitation on the disclosure of prospective data, while acknowledging that a majority of courts to have addressed the government's theory that the *Pen Register Act*, in combination with the *Stored Communications Act*, supports disclosure of prospective cell site location information have denied the government's applications); and *In re U.S. for an Order Authorizing the Use of Two* (Cont'd.)

The Pen Register Act, which authorizes court-ordered electronic monitoring of non-content telephone calling activity, can be used to obtain prospective calling activity information.[93] The Pen Register Act authorizes the installation of pen register and trap and trace devices in both criminal investigations and also in national security investigations pursuant to the Foreign Intelligence Surveillance Act (FISA).[94] Pen registers identify outgoing dialed telephone numbers, while trap and trace devices identify incoming telephone numbers. Pen registers and trap and trace devices require court orders (pen/trap orders) and are issued for a fixed period of time, not to exceed 60 days.

B. Hot Number [redacted]

We found that Company A and Company C [redacted] During the period covered by our review, the FBI identified 87 "hot numbers" for Company A to [redacted] and at least 65 hot numbers for Company C to [redacted]. The FBI did not provide legal process to Company A or Company C either before or after it identified the numbers and received calling activity information.

We describe below details about the FBI's acquisition of this information, what the CAU Unit Chiefs and attorneys in the FBI Office of the General

---

Pen Register and Trap and Trace Devices, 632 F. Supp. 2d 202, 207 (E.D.N.Y. 2008) (granting prospective cell site location information and stating the *Stored Communications Act* does not preclude the ongoing disclosure of records to the government once they are created.

Recent cases have questioned whether any cell site location information – historical or prospective – is available under the *Stored Communications Act*, or whether cell site location information is excluded because the cell phone is then a "tracking device' excluded under the Act. The W.D. Pa. decision has been appealed, and the 3rd Circuit's ruling will be the first appellate decision on the issue. Prior to the appeal to the 3rd Circuit, the Department of Justice concluded that prospective cell site location information was encompassed within the terms of the FISA pen register provision, as amended by the Patriot Reauthorization Act. However, the Department is awaiting the 3rd Circuit's decision before pursuing this position with the FISA Court.

[93] The Pen Register Act, which is part of the ECPA, authorizes the FBI to obtain court orders for the real-time interception of outgoing or incoming telephone numbers to a target telephone. See *Electronic Communications Privacy Act of 1986*, Title III ("Pen Register Act"), Pub. L. No. 99-508, codified as amended at 18 U.S.C. §§ 3121 – 27 (2000 & Supp. 2002). In criminal cases, the courts are authorized to enter ex parte orders for pen registers or trap and trace devices upon certification that the information likely to be obtained "is relevant to an ongoing criminal investigation." 18 U.S.C. § 3122(b)(2).

[94] See 18 U.S.C. §§ 3121 – 27; 50 U.S.C. § 1842(e).

Counsel (FBI OGC) knew about the practice, and our analysis of this practice.

1. Company C

Company C's hot number [redacted] feature was described in a May 23, 2003, proposal of work that led to a contract between the FBI and Company C for the provision of Company C's on-site services in the CAU. A CTD Electronic Communication (EC) dated May 28, 2003, that requested funding for this contract stated that the "statement of work also allows for the [redacted]"[95] However, we found that the FBI did not establish any procedures, guidance, oversight, or training for CAU personnel regarding the use of hot number [redacted] We also found no evidence that NSLB attorneys conducted any legal review of the proposed Company C contract in 2003, including the legal implications of hot number [redacted] Further, we found no evidence that FBI attorneys evaluated the legal implications of hot number [redacted] after Company C posted its on-site employee in the CAU in April 2004, or thereafter, until 2007.[96]

A CAU SSA told us that to obtain information on targeted numbers he provided a list of telephone numbers to Company C [redacted] Company C would then notify him of calling activity by the targeted numbers. The on-site Company C's employee's log indicates that in some instances the Company C employee provided more information than just the fact of calling activity, such as call originating and terminating information.

A Company C representative confirmed for us that Company C did not receive legal process from the FBI to initiate any hot number [redacted] and also did not receive legal process after it had provided information to the FBI about the hot numbers. The Company C representative also said that Company C could not determine how often the feature was used or [redacted] at the request of the FBI during the 4-year period covered by our review. However, based on information provided to us by a CAU SSA who used the Company C service and our review of Company C documents, we estimated that the FBI asked Company C to [redacted] for at least 65 telephone numbers between May 2004 and September 2006.

---

[95] The EC was initiated by the CAU and was approved by Thomas Harrington, the Deputy Assistant Director of the CTD.

[96] As described below, we found that based on inaccurate information provided to her in April 2007, FBI General Counsel Caproni came to the erroneous conclusion that hot number [redacted] had not been used by the CAU.

Company C records also show that the FBI was billed for and paid a separate fee to Company C for this hot number [redacted] We found that the FBI paid Company C [redacted] for hot number [redacted] during the period from 2002 through 2006.[97]

2. Company A

Documents that Company A provided to the FBI as part of Company A's 2004 contract proposal for on-site services in the CAU described Company A's capability to "track, follow, and capture fugitives, terrorists and other criminals" and [redacted] to search for known fugitives (i.e. [redacted] . . . ." One of Company A's stated goals in the proposal was to create a report "to be customized specifically for the FBI based upon input data such as hot target list, significant numbers, secure data, etc."

An on-site Company A analyst told us that Company A's [redacted] capability was [redacted] Company A [redacted] He said he could not recall when information on "hot numbers" was requested by the CAU.[98] Use of this capability enabled the FBI to learn in [redacted] that there was calling activity by the hot numbers. Additionally, if specified by the FBI requesters, Company A would [redacted] the requesters only to calling activity within certain parameters, such as calls to or from a particular area code [redacted] The on-site Company A analyst said that while he received details of the calling activity by the hot numbers – including the date, time, and duration of the calls – he informed the FBI requesters only that there had been calling activity. The Company A analyst told us that he typically notified the CAU or other FBI requesters of the calling activity verbally.

The on-site Company A analyst who set many of the Company A hot number [redacted] told us that he did not discuss with anyone in the FBI or Company A whether legal process would be served before he provided calling activity information. He also said that he did not receive any type of legal

---

[97] Company C's schedule of payments shows that Company C billed the FBI at a rate of [redacted] per month in fiscal year (FY) 2006 for [redacted] for a maximum of 1,000 telephone numbers. A Company C representative told us that Company C also billed the FBI at a flat rate in FY 2002 and FY 2004.

[98] Company A's [redacted] was different from another Company A capability called "hot number [redacted]." Hot number [redacted] permits Company A to collect all toll billing records at set intervals, such as every 4, 8, or 12 hours, while [redacted] provided [redacted] information about calling activity on particular telephone numbers. Company A told us that the FBI never received information or records from Company A in connection with its "hot number [redacted]" service, and we found no contrary evidence.

process or exigent letters for the calling activity information that he provided to the FBI.

Based on information we obtained from Company A, we found that from June 2005 until December 2006, FBI personnel asked Company A to [redacted] for at least 87 telephone numbers. A Company A representative told us that of the 87 telephone numbers, 42 telephone numbers generated calling activity information. The attorney stated that information [redacted] was conveyed to the Company A analyst [redacted] of the calling activity. A CAU SSA who used the [redacted] feature told us that typically he did not receive notification of the calling activity generated on his hot numbers [redacted], usually through an e-mail from the on-site Company A analyst.

Unlike Company C, Company A provided its hot number [redacted] service as part of its overall contract for services to the FBI, and Company A did not impose separate charges for setting hot number [redacted]

A CAU SSA told us that CAU Unit Chief Rogers told him to use Company A's and Company C's hot number [redacted] service in connection with the [redacted] fugitive investigation being conducted by the FBI's [redacted] Field Division and in connection with another fugitive investigation being conducted by the FBI's [redacted] Field Division.[99] Related to the [redacted] investigation, the SSA recalled attending a "meet and greet" session with a [redacted] Field Division supervisor in the CAU that was also attended by CAU Unit Chief Bassem Youssef. The SSA said that the purpose of the meeting was for the CAU to describe its resources and how the CAU could support the [redacted] fugitive investigation.[100] Several months after this meeting, the FBI began identifying hot numbers associated with the [redacted] investigation and giving them to the on-site Company A analyst. The Company A analyst thereafter notified both the CAU SSA and the [redacted] Field Division case agent by e-mail [redacted] of the telephone numbers.

---

[99] The CAU SSA told us that several other CAU personnel used the hot number [redacted] feature in other FBI investigations. We received independent information that corroborated the CAU SSA's statement regarding other CAU personnel using the hot number [redacted] for other CAU cases.

[100] [redacted]

The CAU SSA said that if the case agent was interested in obtaining toll billing records or subscriber information on the hot numbers, the FBI would issue administrative subpoenas or exigent letters for those records.[101] The CAU SSA estimated that he gave Company A a total of 20 telephone numbers in connection with both the [redacted] and the other fugitive investigation.[102]

In our investigation, we found no evidence that the FBI established procedures, guidance, oversight, or training to ensure that CAU personnel sought appropriate legal authority when they asked Company A or Company C to provide calling activity information in response to the FBI's requests [redacted] on hot numbers.

C. FBI OGC and CAU's Unit Chiefs' Knowledge of Hot Number [redacted]

In this section we examine what CAU Unit Chiefs and FBI OGC attorneys knew about hot number [redacted]

CAU Unit Chiefs and FBI OGC attorneys told us they were unaware of the use of hot number [redacted] by CAU personnel. CAU's first Unit Chief, Glenn Rogers, said he thought Company A offered a hot number [redacted] capability [redacted] However, Rogers said he was not certain whether Company A's hot number [redacted] was ever utilized by the FBI and also was not certain what authority the FBI would use to acquire the calling activity information.

---

[101] The CAU SSA told us that before notifying FBI requesters of calling activity by the hot numbers, Company A used "sneak peeks" to first determine whether the calling activity was associated with [redacted] have investigative value. After the Company A analyst made this determination, he notified the FBI of calling activity by telephone numbers that might be of investigative interest.

[102] The CAU SSA said he recalled first learning about hot number [redacted] at a meeting in 2004 he attended with CTD Section Chief Michael Fedarcyk, CAU Unit Chief Rogers, and a female NSLB attorney whose name he could not recall. He stated that they discussed the use of "forward-looking subpoenas" or "anticipatory search warrants" that would request information [redacted] The CAU SSA told us that the NSLB attorney said that she approved of forward-looking subpoenas. He said he was not certain whether the legal processes discussed at the meeting were grand jury subpoenas or NSLs, but that the NSLB attorney said that there was no legal problem with forward-looking subpoenas. He also said that no FBI attorneys ever told him that they had legal reservations about hot number [redacted] We could not identify any NSLB attorney at this meeting, and the FBI could not locate documentation of any legal review by the NSLB of hot number [redacted] or other features of the Company A contract from 2003 through 2007.

Rogers's successor as CAU Unit Chief, Bassem Youssef, told us that hot number [redacted] was a feature offered by Company C whereby the FBI "would have authority on a particular target number" [redacted] However, Youssef said he did not know what the authority was for hot number [redacted] He said that after making inquiries with an FBI field division in 2006 and 2007, he believed that the FBI had never used Company C's hot number [redacted] capabilities.

On September 12, 2006, a CTD Contracting Officer's Technical Representative (COTR) sent an e-mail to Youssef asking him whether the CAU still needed Company C's hot number [redacted] service for which the FBI was then paying [redacted] per month.[103] Youssef responded that he no longer needed the hot number [redacted] feature and, in the event it were needed in the future, "we would ask for it on a month to month basis." The COTR asked Youssef to contact Company C and let it know that the FBI was cancelling the service.

On September 18, 2006, Youssef informed the Company C on-site employee by e-mail that "we no longer need the hot # [redacted] feature and we'll re-institute it in the future if we need it again." The Company C employee replied by e-mail that Company C was then using the feature for two FBI investigations: the [redacted] fugitive investigation being conducted by the FBI's [redacted] Field Division and a second fugitive investigation being conducted by the [redacted] Field Division. The Company C employee asked Youssef to confirm that he wanted to terminate hot number [redacted] for both investigations, which Youssef confirmed.

Marion Bowman, who was the National Security Law Branch (NSLB) Deputy General Counsel when the contracts were executed, told us that he was unaware of and did not review the contracts with Company A, Company B, or Company C to provide on-site services at the CAU and did not know the specifications for the contracts. Bowman's successor as NSLB Deputy General Counsel, Julie Thomas, told us that she recalled reviewing the contracts with the on-site providers for the first time in late 2006, after receiving a draft of the OIG's first NSL report. She stated that she recalled identifying the provision of the contract discussing hot number [redacted] and concluding that the FBI could obtain this type of information only through a pen register. She said that

---

[103] Youssef had co-signed the Company C monthly invoices that included charges for this feature for 12 consecutive months prior to the COTR asking him whether Company C's hot number feature was needed. However, the invoices only referenced a lump sum amount and did not itemize the particular services provided for the charges.

she also recalled learning in April 2007 that Caproni had been informed at that time that the service had never been used. Thomas said she did not learn until shortly before her final OIG interview for this report in August 2008 that the FBI had paid Company C for hot number [redacted]

Caproni told us that based on information she had received from FBI personnel in April 2007, she believed that hot number [redacted] had never been used by the FBI. In an April 2007 e-mail to CTD Assistant Director Joseph Billy, Jr., and other CTD personnel, Caproni instructed that if the CTD sought to use hot number [redacted] CTD must first contact the FBI OGC. She added that the FBI OGC needed to understand the technical aspects of the feature before providing a legal opinion about its use. In 2008, Caproni told us that her concern at the time was that the feature "might be an unlawful pen register."[104]

D. OIG Analysis

We found that the FBI sought calling activity information on 152 "hot" telephone numbers from Company A and Company C and was provided information on at least 42 of those numbers. Company A provided information that there had been calls made to or from the numbers identified by the FBI, sometimes in response to specific inquiries from the FBI about whether calling activity existed to or from a particular area code [redacted] We also found evidence that Company C also may have provided more information than just the existence of calling activity, such as call originating and termination information.

We believe that the calling activity information requested by and conveyed to the FBI about these hot numbers required legal process. Although the information given to the FBI by Company A and Company C on these hot numbers was less extensive than the type of information typically provided in response to NSLs or pen register/trap and trace orders, it constituted "a record or other information pertaining to a subscriber or a customer" under the ECPA.[105]

As discussed in Chapter Two of this report in connection with our analysis of "sneak peeks," the Department's Office of Legal Counsel concluded, and we agree, that the ECPA ordinarily bars communications service providers

---

[104] After reviewing a draft of this report, the FBI stated that, subsequent to her OIG interview, Caproni concluded that as a matter of law, hot number [redacted] did not implicate the Pen Register Act.

[105] 18 U.S.C. § 2702(a)(3).

from telling the FBI, prior to service of legal process, whether a particular account exists. We also concluded that if that type of information falls within the ambit of "a record or other information pertaining to a subscriber to or customer of such service" under 18 U.S.C. § 2702(a)(3), so does the existence of calling activity by particular hot telephone numbers, absent a qualifying emergency under 18 U.S.C. § 2702(c)(4).

We found no evidence that the FBI requested or the providers gave the FBI this information pursuant to the emergency voluntary disclosure provision of the ECPA. Instead, it appears that the information was disclosed as part of the contractual arrangement between the providers and the FBI, and was primarily used in connection with fugitive matters that did not qualify as emergency situations under 18 U.S.C. § 2702. Therefore, we believe that the practice of obtaining calling activity information about hot numbers in these matters without service of legal process violated the ECPA.

We also found it both surprising and troubling that Rogers, as Unit Chief of the CAU and the official responsible for knowing and assessing the tools used by his subordinates to obtain information from the on-site providers, said he was not certain whether Company A's hot number [redacted] feature was ever utilized by the FBI. We likewise were troubled that Youssef, Roger's successor as CAU Unit Chief, told us that he did not believe that hot number [redacted] was used.

In addition, from the inception of the FBI's contractual relationship with the three providers beginning in 2003, senior FBI officials knew that the CAU would be handling telephone transactional records which the FBI could lawfully obtain pursuant to the ECPA. However, the FBI failed to ensure that responsible officials in the CTD and the FBI OGC's NSLB reviewed the proposed and final contracts with the providers to ensure that the agreements conformed to the requirements of the ECPA and other relevant laws and policies. The General Counsel and the NSLB Deputy General Counsel did not review the contracts or associated documents with the on-site providers until late 2006 or early 2007. We believe that the absence of timely legal review was a significant management failure by the FBI. In part because NSLB attorneys did not review the contract proposals with the on-site providers, they were unaware of the specific services provided, including the hot number [redacted] service.

In Chapter Six of this report we provide recommendations to address our findings from this portion of our review. We believe the FBI should carefully review the circumstances in which FBI personnel asked the on-site communications service providers [redacted] "hot numbers" to enable the Department to determine if the FBI obtained calling activity information under circumstances that trigger discovery or other obligations in any criminal investigations or prosecutions. Our recommendations also are

designed to ensure that FBI personnel receive periodic training on the FBI's authorities to obtain telephone records from communications service providers and that FBI OGC attorneys and program managers, including successor officials serving in these positions, are fully familiar with any FBI contracts with communications service providers.

II. Seeking Reporters' Telephone Records Without Required Approvals

We determined that in three media leak investigations the FBI requested, and in two of these instances obtained from the on-site communications service providers, telephone records or other calling activity information for telephone numbers assigned to reporters. However, the FBI did not comply with the federal regulation and Department policy that requires Attorney General approval and a balancing of First Amendment interests and the interests of law enforcement before issuing subpoenas for the production of reporters' telephone toll billing records.[106]

In the sections that follow, we describe the federal regulation and Department policies governing the issuance of subpoenas for the telephone toll billing records of members of the news media, the facts we found regarding each of these three leak investigations, and our analysis of each of these three cases.

A. Federal Regulations and Department Policies

Because of the First Amendment interests implicated by compulsory process to obtain reporter's testimony or their telephone records, 28 C.F.R. § 50.10 (2004) requires special approvals and other advance steps before Department employees are permitted to issue subpoenas for reporters' testimony or the production of their telephone records.

Specifically, this regulation requires that before issuance of such subpoenas, "all reasonable attempts should be made to obtain information from alternative sources."[107] This regulation also requires the Department to attempt to negotiate the voluntary appearance of the news media personnel or the voluntary acquisition of their records. If the records are needed for a criminal investigation, the regulation requires "reasonable grounds to believe, based on information obtained from non-media sources, that a crime has

---

[106] See 28 C.F.R. § 50.10.

[107] 28 C.F.R. § 50.10(b).

occurred, and that the information sought is essential to a successful investigation . . . ."[108] Any requests for such subpoenas must be approved by the Attorney General in accordance with principles specified in the regulations.[109]

The regulation also requires that if the telephone toll records of members of the news media are subpoenaed without the required notice, the affected member of the news media must be notified "as soon thereafter as it is determined that such notification will no longer pose a . . . substantial threat to the integrity of the investigation" and, in any event, within 45 days of any return in response to the subpoena.[110] Finally, the regulations state that failure to obtain the prior approval of the Attorney General "may constitute grounds for an administrative reprimand or other appropriate disciplinary action."[111]

Department policies supplement this regulation by specifying the information required to be included in requests seeking Attorney General approval for issuance of such subpoenas.[112]

At the time of the investigations at issue, the FBI's media leak investigations were governed by the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations.[113] In addition, at the time of these investigations, leak investigations involving

---

[108] 28 C.F.R. § 50.10(f)(1).

[109] 28 C.F.R. § 50.10(g).

[110] Section 50.10(g)(3) of 28 C.F.R. states:

> When the telephone toll records of a member of the news media have been subpoenaed without the notice provided for in paragraph (e)(2) of this section, notification of the subpoena shall be given to the member of the news media as soon thereafter as it is determined that such notification will no longer pose a clear and substantial threat to the integrity of the investigation. In any event, such notification shall occur within 45 days of any return made pursuant to the subpoena, except that the responsible Assistant Attorney General may authorize delay of notification for no more than an additional 45 days.

[111] 28 C.F.R. § 50.10(n)(2004).

[112] See United States Attorneys' Manual § 9-13.400, "News Media Subpoenas; Subpoenas for Telephone Toll Records of News Media; Interrogation, Arrest, or Criminal Charging of Members of the News Media."

[113] As noted previously, several sets of Attorney General Guidelines were revised and consolidated into the Attorney General's Consolidated Guidelines, which took effect in December 2008.

classified information were categorized by the FBI as espionage investigations because they potentially involved violations of the Espionage Act.

B. First Matter

1. Background

[redacted] An FBI squad supervisor told us that in response the FBI CTD opened a counterterrorism investigation into [redacted]

[redacted] the Washington Post and The New York Times published articles [redacted][114] The Washington Post article referred to [redacted] indicating that, [redacted] The New York Times article referred to information from a [redacted] given to FBI investigators about [redacted]

2. The Investigation of the Leak of Information to the Media

The FBI's [redacted] Field Office initiated a leak investigation [redacted] to determine whether U.S. government employees or others had violated criminal laws prohibiting the release of classified information in connection with the Washington Post and The New York Times articles. The investigation was assigned to a [redacted] Field Office counterintelligence squad, and a case agent was assigned to the matter. The U.S. Attorney's office in [redacted] assigned an Assistant United States Attorney (AUSA) to the investigation on or about October [redacted].

---

[114] [redacted]

According to our interviews and review of FBI documents, in November [redacted] the AUSA assigned to the investigation discussed with the FBI case agent the possibility of seeking Department approval to subpoena the telephone toll billing records of the reporters who wrote the two articles in the Post and the Times. The case agent and the AUSA told us that they were both aware at that time of the Department's regulation that requires Attorney General approval for obtaining reporters' telephone toll records, and they recalled discussing the possibility of seeking such approval. They both stated that before taking this step they believed they should determine whether the toll billing records of [redacted] calls made by the reporters and others [redacted] could be obtained from the on-site communications service providers located in the CAU.

a. The [redacted] Field Office Requests CAU Assistance

On November 5, [redacted], the case agent sent an e-mail asking another Special Agent in the [redacted] Field Office to inquire, in the other agent's capacity as his squad's liaison to the CAU, whether the on-site communications service providers could obtain telephone toll records of U.S. persons making [redacted] calls [redacted]. The case agent's November 5 e-mail listed 12 [redacted] telephone numbers, 8 of which were identified in the e-mail as belonging to Washington Post reporters [redacted] and Washington Post researcher [redacted] and New York Times reporters [redacted] The e-mail identified a 7-month time period – a few months before and a few months after the published articles – as the time period of interest for the leak investigation.

Three days later, the Special Agent who had received the e-mail from the case agent forwarded the e-mail to a CAU SSA – also copying the case agent. The Special Agent asked the CAU SSA in his forwarding e-mail whether, as a general matter, [redacted] calls generated by the identified telephone numbers originating [redacted] would be captured by the on-site providers' systems.

The CAU SSA replied by e-mail on November 10, [redacted], asking whether the Special Agent wanted him "to start pulling these tolls" and, if so, "what is the source of the request . . . NSL or FGJ subpoena?" The CAU SSA's e-mail was copied to the case agent's supervisor, but not to the case agent.

We found no e-mail response to the CAU SSA's questions, either from the Special Agent or anyone else. When we asked the Special Agent about this e-mail, he told us that he did not recall it.

In September and December [redacted], a CAU SSA and other CAU personnel provided briefings to the [redacted] Field Office's [redacted] squads, including the case agent assigned to the leak investigation (who attended one of the briefings), about the resources available to support FBI investigations from the on-site communications service providers.

Five days after the December [redacted] briefing, the case agent on the leak investigation sent an e-mail to a CAU Intelligence Analyst who had participated in the briefing, asking the same questions that had been previously posed to the CAU SSA by the Special Agent: could the on-site providers obtain toll records on [redacted] calls originating [redacted] telephone numbers [redacted] The case agent stated in his December 14 e-mail to the CAU Intelligence Analyst, "You suggested that we run this past you before we send the subpoena." The e-mail also stated, "We likely will proceed with a federal grand jury subpoena, with the AUSA requesting DOJ approval before issuing the subpoena." The case agent also noted in the e-mail that the Special Agent who had originally forwarded this request to the CAU had already "touched base with [the CAU SSA] preliminarily on this matter."

In response, on December 14, [redacted], the CAU Intelligence Analyst sent the case agent a sample NSL for toll billing records. The Intelligence Analyst also stated in his e-mail that he would check with the CAU SSA "to make sure he hasn't already pulled the tolls." We found no evidence indicating that the CAU SSA received this e-mail or that he was informed about any planned request for DOJ approval.

However, in the absence of any request from the case agent or anyone in the FBI, the CAU SSA issued an exigent letter dated December 17, [redacted], to Company A for telephone records of the reporters and others listed in the case agent's November 5, [redacted], e-mail. We determined that the SSA did this without further discussion with the case agent or the Special Agent who had asked only whether such records could be obtained through the on-site providers, not that the records should be obtained.[115]

The CAU SSA's exigent letter sought records on nine telephone numbers, seven of which were identified in the e-mail exchanges described above as belonging to Washington Post and New York Times reporters or their news organizations' bureaus in [redacted] The other two numbers were associated

---

[115] We determined that this SSA had issued a total of 115 exigent letters, the second highest number of exigent letters signed by any CAU personnel.