unaware of exigent letters until he read press accounts in 2007 about the OIG's first NSL report. Similarly, Willie Hulon, who served as Assistant Director of the CTD from December 2004 to June 2006, and as Executive Assistant Director for the FBI's National Security Branch from June 2006 to January 2008, told us that he did not know about exigent letters. Hulon said he "assumed that we were using the NSL legal process." Joseph Billy, Jr., who served as one of the CTD's Deputy Assistant Directors from April 2005 to October 2006, as its acting Assistant Director from June 2005 to October 2006, and as its Assistant Director from October 2006 until his retirement from the FBI in March 2008, also told us that he did not know about the CAU's use of exigent letters until the OIG's first NSL investigation discovered the practice in 2006.

D. The FBI's Senior Leadership

The FBI's senior leadership also told us they were unaware of the CAU's use of exigent letters until the OIG's first NSL investigation.

We determined that in July 2006, shortly after OIG investigators conducted the first interviews in our first NSL review, FBI General Counsel Valerie Caproni was informed by the Assistant General Counsel that in emergency circumstances the CAU was using letters that promised future legal process to obtain records from the on-site providers. The Assistant General Counsel also advised Caproni that there had been problems with identifying preliminary investigations to which after-the-fact NSLs could be tied, but that NSLs were being issued within 2 or 3 days. However, Caproni told us that she did not actually see an exigent letter until December 2006 when the OIG showed her some sample exigent letters during an interview in connection with our first NSL report.

FBI Deputy Director John Pistole served as Deputy Assistant Director and then Assistant Director of the CTD from May 2002 to October 2004, and as Executive Assistant Director of the National Security Branch from December 2003 to October 2004. Pistole told us that he did not know specifically about the use of exigent letters. He said he understood that if something was "hot, you could get the information right away and then follow up with paper," which was the "normal course of business" in counterterrorism investigations.

FBI Director Mueller told us that he was unaware of the CAU's use of exigent letters until at or about the time the FBI received the draft of the OIG's first NSL report, which was in late 2006. Mueller stated that, until then, he was unaware that the CAU was receiving telephone records without the appropriate legal process.

E. Employees of On-site Communications Service Providers

We also interviewed employees of the communications service providers who were assigned to the FBI about the use of exigent letters.

The first Company A analyst who arrived at the CAU in April 2003 told us that he was acquainted with the use of exigent letters from his previous experience as an on-site analyst at the FBI's New York Field Division, where, as noted above, exigent letters had been in use since 2002. Rogers and other CAU personnel who signed exigent letters said that this Company A analyst told them that exigent letters were a method for requesting telephone records from Company A. This analyst defined exigent circumstances as "needing of the records immediately." The Company A analyst confirmed that he often informally briefed CAU and other FBI personnel on the use of exigent letters, and said he told them that they could use an exigent letter when "they needed the records quicker."

The on-site Company C employee, who arrived at the CAU in April 2004, told us that neither his company supervisors nor FBI officials described exigent letters to him before he began working at the CAU. He said that he was first presented with an exigent letter soon after his arrival at the CAU and that he accepted the legitimacy of the letter based on the "credibility" of both the SSA who signed the exigent letter and "the whole unit."[47] The Company C employee, who did not have prior experience in subpoena or NSL compliance, told us that he accepted exigent letters at "face value" as indicating that the FBI needed the data as soon as possible and would subsequently provide legal process. The Company C employee stated that he honored exigent letters without consulting his Company C supervisors.

The on-site Company B employee arrived at the CAU in early September 2004. This employee had extensive prior experience with subpoena compliance. He said he had not been told prior to his arrival about the CAU's use of exigent letters, and that on the second day of his assignment, September 8, 2004, a CAU intelligence analyst presented him with an exigent letter. The Company B employee said he initially declined to honor the exigent letter, telling the CAU analyst that she would need to provide an NSL before Company B would process the request. The Company B employee stated that the analyst was "stunned" by his refusal

---

[47] The first exigent letter we found that was issued to the on-site Company C employee was dated April 14, 2004.

and took the matter to a CAU SSA. The Company B employee said the CAU SSA then explained to him the concept of exigent letters and told him the NSL was "not written or not going to be written right now or today." The Company B employee told us that he conferred with his Company B supervisor, who told him to honor the requests but to be sure to get the after-the-fact legal process. Thereafter, the Company B employee regularly accepted exigent letters and provided responsive records to the CAU. The Company B employee told us that "the majority of the time" he "did not know what the [exigent] circumstance was." He said he "pretty much assumed . . . that it was an exigent circumstance" because he was supporting counterterrorism investigations in the CAU.

We determined that the providers' on-site employees often received exigent letters from CAU personnel – and responded to them – without receiving any information about the FBI investigations for which the records were needed. The providers' employees told us that they accepted exigent letters without question and assumed that the circumstances were exigent. For example, the Company C employee told us, "most of the time I know nothing about the case personally" and that he sometimes relied on CAU personnel saying the matter was "hot." The Company B employee said that he only received case details related to exigent letter requests less than 25 percent of the time, but he reasoned each time that, "it is an emergency situation and they need my assistance. I am taking their word." A Company A analyst told us that the CAU requesters "did not always tell me the circumstances of why they needed the records" and said he accepted the FBI's representation in the exigent letters, observing, "personally, it wasn't my place to police the police."

The Company B employee told us that although he "assumed" CAU's requests were emergencies, he had concerns about whether the exigent letter requests were truly emergencies, and these concerns led in part to Company B's decision to change its procedures. Beginning on October 10, 2006, the on-site Company B employee placed a stamp on the exigent letters for which he provided responsive records. The stamped text stated, "An emergency involving danger of death or serious physical injury to a person requires disclosure without delay of information relating to the emergency."[48] The Company B employee told us that he added the stamped text to the exigent letters at the direction of Company B's legal counsel and he also required FBI requesters to certify by initialing and dating the stamped declaration that the circumstances of the request comported with

---

[48] The stamp appeared on the final 13 exigent letters served on the on-site Company B employee between October 10, 2006, and November 6, 2006.

the legal standard for an emergency voluntary disclosure pursuant to 18 U.S.C. § 2702(c)(4).[49] The Company B employee stated that he did not provide responsive records unless requesters signed or initialed this certification.

The Company B employee told us that he also followed his supervisor's instruction to be sure to get after-the-fact legal process, and he: (1) created a spreadsheet to track the outstanding legal process; (2) reminded CAU personnel and sometimes requesters in the field via either face-to-face conversations, telephone calls, or e-mails that he was still awaiting process; (3) brought the issue of exigent letters to the attention of CAU Unit Chief Glenn Rogers and later Unit Chief Bassem Youssef; and (4) provided a list of telephone numbers still awaiting process to a CAU SSA so that the numbers could be incorporated into the Company B May 12, 2006, "blanket NSL" described in Chapter Four.

F. Types of Cases in which Exigent Letters were Used

CAU agents, analysts, and Unit Chiefs told us that they used exigent letters and other informal requests to the on-site communications service providers to quickly obtain telephone records and analyze them in connection with many urgent, high priority counterterrorism investigations. They said that many of the requests that came to the CAU involved telephone numbers from [redacted]

---

[49] 18 U.S.C. § 2702(c)(4) provides:

Voluntary disclosure of customer communications or records.

* * *

(c) Exceptions for disclosure of customer records. – A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2)) . . . .

* * *

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency; . . . .

An earlier version of this provision that was in effect between 2003 and March 8, 2006 – the period when most of the exigent letters were issued – authorized a provider to voluntarily release toll records information to a governmental entity if the provider "reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information."

[redacted] Large groups of telephone numbers were [redacted] and the FBI moved quickly to exploit the numbers, [redacted] and that might reveal links to possible terrorist activities [redacted]

According to FBI officials, on some occasions the CAU sought telephone records in connection with international terrorism investigations involving terrorist plots that were believed to pose an imminent threat to the United States or its citizens abroad. For example, in a [redacted] case that received widespread media attention, the FBI investigated a terrorist plot [redacted] to detonate explosives [redacted] CAU personnel sought calling records for thousands of telephone numbers in support of this investigation, which we refer to as Operation Y in this report. CAU personnel also said they used exigent letters to obtain calling information to help the FBI address numerous bomb threats. FBI officials said that in these and other cases the CAU enabled the FBI to quickly address serious threats through its ready access to the on-site communications service providers.

The CAU also used the on-site communications service providers to obtain telephone records in support of criminal investigations, such as organized crime and kidnapping cases. For example, the CAU issued exigent letters in the kidnapping investigations regarding [redacted] who disappeared in 2005 [redacted] and [redacted], a U.S. citizen from [redacted] who was kidnapped in Iraq [redacted]

However, as described in Chapters Four and Six, FBI officials told us that the investigations for which exigent letters were used, although urgent and important, did not necessarily involve imminent threats or life-threatening circumstances. For example, we discuss in Chapter Four a high-profile FBI operation we call "Operation Z" for which CAU personnel used exigent letters and other informal requests to request records for hundreds of telephone numbers associated with a dead terrorist. According to the FBI supervisors responsible for the operation, the circumstances in which the records were obtained for exploitation were not exigent. In addition, we found that exigent letters were issued in cases such as media leak investigations, fugitive investigations, and other investigations that did not include exigent or life-threatening circumstances.

IV. Other Informal Methods for Requesting Records without Prior Service of Legal Process

In addition to the use of exigent letters, we determined that CAU personnel regularly requested and received from the three on-site communications service providers toll records and other information related to [redacted] telephone numbers without issuing any legal process or even providing exigent letters. We could not determine the full scope of this practice since the CAU had no systematic tracking system to document the requests, and the telephone providers did not consistently document these requests. However, based on our interviews of CAU personnel and the providers' employees, as well as our review of documents, we concluded that CAU personnel requested [redacted] for records of more than 3,500 telephone numbers without prior service of legal process or even exigent letters.

A. E-mail, Face-to-Face or Telephone Requests, and Informal Notes

In most of the instances described in this section, CAU personnel conveyed their record requests to the on-site providers by FBI e-mail. However, employees of the providers also told us that CAU personnel sometimes conveyed their [redacted] requests by giving target telephone numbers to the providers' employees verbally during telephone calls or visits to the providers' CAU work stations, or on pieces of paper, such as post-it notes. CAU personnel also sometimes sent requests to the providers' [redacted]

A CAU Intelligence Analyst told us that one of the Company A analysts routinely provided toll records to him without first receiving legal process or an exigent letter. The CAU Intelligence Analyst stated that this was the process he used "close to 100 percent of the time." The Intelligence Analyst said he would usually fax an exigent letter to the Company A analyst several days after he received responsive records pursuant to his informal requests. We also found several FBI documents indicating that on-site Company A employees [redacted] and in many cases provided telephone toll billing records to the FBI without any prior legal process or even exigent letters.

Exigent letters were never provided to Company A for many of these requests, either before or after the fact. Indeed, as we describe in Chapter

Four of this report, the FBI was able to locate exigent letters for only 235 of the 700 telephone numbers listed on one of the so-called "blanket" NSLs issued by the FBI to cover or validate records previously obtained by the FBI.[50]

We did not have similar data for Company B and Company C, but employees of both carriers told us they also [redacted] and provided telephone records to the FBI in response to e-mails and verbal requests and without legal process or exigent letters. The Company B and Company C employees stated that they believed such [redacted] usually related to major FBI counterterrorism investigations.

We also determined that in connection with at least three major FBI counterterrorism investigations in 2005 and 2006, CAU personnel requested telephone records for hundreds of telephone numbers from the three on-site communications service providers. While we identified some exigent letters associated with these operations, the majority of the requests in these operations were initiated without legal process or exigent letters. In a majority of these instances, even when records were turned over to the FBI, exigent letters were not subsequently provided to cover the requests and records provided for these major operations. Moreover, in most instances the FBI issued legal process to cover these requests well after the records had been provided to the FBI, from 20 days later to 6 months later.

The on-site Company C employee also told us that apart from major FBI operations, he occasionally provided records to CAU personnel prior to receiving legal process or an exigent letter. We also reviewed an e-mail message the Company C employee sent in January 2006 to Unit Chief Youssef and a CAU Intelligence Analyst in which the Company C employee stated that he would give priority to requests which did not have accompanying legal process or an exigent letter if the CAU provided him a reason to do so. In response to this e-mail, the CAU Intelligence Analyst stated that "[w]e are working with hundreds of numbers and it's not practical to give the [exigent letter] for every number that comes in."

We also reviewed the on-site Company C employee's log and identified numerous instances apart from major FBI operations where telephone records were provided to the CAU without legal process or exigent letters.[51]

---

[50] This was the Company A September 21, 2006, blanket NSL, described in Chapter Four.

[51] The Company C on-site employee kept a contemporaneous log of requests made by CAU personnel. He said he used the log to record requests for [redacted], including requests pursuant to legal process, exigent letters, sneak peek requests, and, in some (Cont'd.)

In some instances the FBI issued exigent letters after receiving the records. In other instances, exigent letters were never provided or the FBI did not issue any after-the-fact legal process for up to 20 months.

The on-site Company B employee told us that he gave telephone records to the FBI without legal process or exigent letters more often in connection with major FBI operations than in other matters. However, we reviewed e-mails from September 2005 to November 2005 indicating that on at least three occasions the Company B employee provided records to CAU personnel prior to receiving legal process or exigent letters, and none of these three instances related to major operations.

B. "Sneak Peeks" or "Quick Peeks"

Many CAU SSAs and Intelligence Analysts we interviewed, and employees of the three on-site communications service providers, also told us about a practice that became known in the CAU as "sneak peeks" or "quick peeks." At the request of CAU personnel, the providers' employees routinely [redacted] of their databases to determine whether they had any responsive records, without receiving legal process or exigent letters. The providers' employees would then describe for the CAU personnel the information contained in the databases without providing the records to CAU personnel. We reviewed documents showing that employees of all of the on-site providers communicated this type of information to CAU personnel either verbally, by e-mail, or telephonically. At times, the providers' employees even invited CAU personnel to view records on their computer screens. If the providers' databases contained requested records, CAU personnel would then decide whether to issue exigent letters or obtain legal process from the field division or Headquarters' operating unit in order to obtain the actual records.

Glenn Rogers, the CAU's first permanent Unit Chief, acknowledged to us that he knew about this practice of sneak peeks. He stated that he believed the practice was first used in the FBI's New York Field Division before it was used by CAU personnel. He said he did not see any legal problem with the practice and stated it was his understanding that there was no expectation of privacy in telephone records because the "numbers belong to the phone companies." He said he therefore did not think there was anything wrong with requesting sneak peeks, and he did not believe

---

instances, post-it notes or a "sticky." Neither Company A nor Company B maintained similar logs. However, both Company A and Company B are able to retrieve records of the [redacted] by their on-site employees.

that NSLs or other legal processes were required prior to such sneak peeks. Bassem Youssef, who succeeded Rogers as the CAU Unit Chief, told us that he had no "first-hand knowledge" of the sneak peek practice in the CAU during his tenure. However, Youssef stated that the concept, as he came to learn in 2007, was to indicate only whether the on-site providers had responsive records on a telephone number.[52]

We also reviewed the Company C employee's log and identified many entries of database [redacted] for which the employee noted that there was "no paper." The log identified CAU requests such as "any calls between these numbers in past month," "any [redacted] calls during Dec 22-25, 2005 [for three domestic telephone numbers]," and "any [telephone calling] activity [for three domestic telephone numbers]." The Company C employee told us that "sometimes there was nothing said" by FBI personnel about the reasons for sneak peek requests. The requesters sometimes just said, "here is a sticky with numbers" and they would specify a date range.

E-mail records we examined from employees of the three on-site communications service providers also showed that in response to sneak peek requests, they confirmed whether the provider had records on an identified telephone number. These e-mails also showed that the providers' employees sometimes responded to these requests with additional information about the calling activity by the identified telephone numbers. For example, e-mail messages from the providers to CAU personnel often included whether the telephone number belonged to a particular subscriber or a synopsis of the call records, such as the number of calls to and from a specific telephone number within certain date parameters, the area codes [redacted] called, and call duration.[53]

The on-site Company C employee told us that he responded to requests for sneak peeks "fairly frequently," estimating that he responded to such requests approximately 300 times (which represented nearly one-half of all the requests he received from CAU personnel from April 2004 until June 2007). The on-site Company B employee stated that sneak peeks

---

[52] We asked Youssef about an August 8, 2006, entry in the Company C employee's log which listed Youssef as the CAU requester for a sneak peek involving four telephone numbers. Youssef told us that he had no recollection of making such a request to the Company C employee.

[53] As described in Chapter Three of this report, sneak peeks were used by the FBI in connection with a media leak matter in which the three on-site providers [redacted] their databases for calling activity of a reporter.

"could have been 1, 2, or 3 times a week." An on-site Company A analyst told us that sneak peeks occurred daily.

We also reviewed e-mails from CAU personnel to employees of the three on-site providers with requests to [redacted] their databases for specific calling activity. For example, in September 2005 an on-site Company A analyst received an e-mail request from a CAU Intelligence Analyst that listed four domestic telephone numbers and asked:

> Could you take a look at these numbers, below, and let me know if you have any calls to [redacted] or Oregon in the past six months? If so, [FBI case agent] has indicated he will be able to provide us with a subpoena.

Similarly, in a March 2006 e-mail exchange between a CAU Intelligence Analyst and the on-site Company B employee with the subject line "quick peek," the Intelligence Analyst requested a "quick peek to see if [Company B has] any data" for a specific [redacted] cellular phone number. The Company B employee responded to the request, "I ran the number for the past [redacted] days and picked up some calls. Stop by my desk if you'd like to see the calls."

We also reviewed a series of e-mails between CAU personnel and a Company A analyst related to a major counterterrorism investigation that was underway in [redacted] 2006. In one of the e-mails, Unit Chief Youssef provided a list of four telephone numbers that were determined by a prior Company A [redacted] to be in contact with a particular telephone number that had been a target number in an NSL. In response, the Company A analyst wrote to Youssef, a CAU Intelligence Analyst, and a CAU SSA that, based on Youssef's request, Company A took a "quick peek" at the calling activity of the four telephone numbers identified in the earlier e-mail. The Company A analyst wrote, "very interesting calling patterns and we strongly suggest that these numbers are added to the NSL for exploitation."

The evidence indicates that the FBI OGC first learned about sneak peeks in February 2007 when a CAU SSA, at Youssef's direction, sent an e-mail to FBI General Counsel Valerie Caproni, NSLB Deputy General Counsel Julie Thomas, and the Assistant General Counsel in which the SSA addressed various statistics related to the CAU's use of exigent letters such as the total number of exigent letters issued by the CAU, the total number of telephone numbers included in the exigent letters, the number of telephone numbers for which records had been obtained from the providers without legal process or an exigent letter, and the number of telephone numbers for which legal process was required. In this e-mail, the CAU SSA, for no apparent reason, referred to the sneak peek practice. He described the practice as "a process wherein the telecom provider would glance at the

network to check if it was meritorious to draft a subpoena and/or NSL to officially request the records." The e-mail stated that if there were no records, an NSL would not be drafted.

Caproni told us that she did not recall the SSA's e-mail. When we asked her if she was aware that the FBI at times received more information than just whether the provider had records on a particular number, she said she was not.

As discussed in the analysis section at the end of this chapter, we concluded that the FBI's use of these sneak peeks in many cases violated the ECPA.

V. Records Obtained in Response to Exigent Letters and Other Informal Requests

In this section, we describe the types of records obtained by the FBI from the on-site communications service providers in response to exigent letters and other informal requests. We also discuss how these records were analyzed and uploaded into FBI databases. In addition, we describe "community of interest" or "calling circle" [redacted] (often called a community of interest"), through which Company A [redacted]

A. Types of Records Collected by the Providers

Each of the three on-site communications service providers had different capabilities to respond to the CAU's requests for telephone records.

[redacted]

The amount of information available to the FBI under its contract with Company A was substantial. PowerPoint slides prepared by Company A explaining its resources, which were incorporated into a CAU presentation

for other FBI divisions and units, stated that Company A [redacted] The slides stated that Company A [redacted]

- domestic [redacted]
- local and long distance calls;
- [redacted]
- [redacted]
- cellular calls, [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Of the three providers, Company A had the greatest volume of records available to the FBI. The key features of Company A's on-site support were the availability of [redacted] of telephone records, [redacted] These features were not available to FBI field agents or Headquarters personnel who served NSLs on Company A through its more formal procedures.

The on-site Company C employee also had access to calling records of telephone [redacted]

[redacted], the Company B on-site employee could only provide calling records [redacted] These were the same types of telephone records that FBI agents outside of the CAU obtained from Company B's

subpoena compliance office. The records available to Company B's on-site employee dated back [redacted][54] Nevertheless, like the advantage offered by the Company A and Company C on-site employees, the advantage offered by the on-site Company B employee was the speed with which requests to Company B were processed and records provided to the CAU.

Employees of the three on-site communications service providers told us that they believed that they could release any information in their databases to the FBI without regard to whether the request was documented in exigent letters, NSLs, or grand jury subpoenas.

B. How Records were Uploaded and Analyzed by the FBI

CAU personnel told us that the three on-site communications service providers delivered telephone records to the CAU in an electronic format that was compatible with FBI databases and a [redacted] database used by the FBI primarily for analysis of telephone toll billing records. The records provided in electronic format could be directly uploaded without being re-formatted. The on-site communications service providers' employees told us that during normal business hours they usually hand-delivered to CAU employees the requested electronic records on a compact disk (CD). In many instances the on-site providers' employees would also contemporaneously forward an electronic copy of the records to the CAU requesters as e-mail attachments.

We found that in [redacted] the on-site providers sometimes forwarded telephone records to CAU requesters [redacted] Some of these records sent to CAU requesters [redacted] were associated with high-value terrorists.[55]

---

[54] Although the FBI's requirements for the Company B contract stated that Company B "would deliver at least [redacted] of historical records," the on-site Company B employee told us that in some instances he was able to obtain records for up to [redacted]

[55] The OIG informed the FBI Inspection Division about this practice and raised concerns about possible breaches of FBI internal policies, as well as security concerns raised by the [redacted] The Inspection Division informed us that the telephone [redacted] did not contain any classified information and that the CTD did not consider the matter to be a security issue. We disagree, and believe that [redacted] does raise security concerns.

We also determined that the telephone records received by the CAU were routinely uploaded into the [redacted] database without being compared to the FBI's original request. The CAU employee in charge of the CAU team that uploaded the records told us that there was no mechanism in place to verify that the records were for the target telephone numbers and within the date ranges specified in the original request. He also stated that his team did not receive a copy of the FBI's original request. The team therefore was not in position to check whether any information had been mistakenly supplied to the FBI or had been mistakenly requested due to FBI errors. Several CAU SSAs and Intelligence Analysts told us that they sometimes informally checked the records to see whether the records matched the requests, but none of these individuals said there was any formal protocol requiring such a review.[56]

After the CAU team uploaded the records to the [redacted] database, a CAU employee would deliver the CD to the CAU requester, who was responsible for forwarding the CD to the FBI field or Headquarters' operating unit that had initiated the request. The CD containing records was considered by the CAU to be the "original" evidence.

[redacted]

The results of the CAU's analysis are used to create documents called "trace reports" or "[redacted] reports" that were normally forwarded to requesters as attachments to an EC. However, field office requesters sometimes preferred to conduct their own analysis and would specify that the CAU not perform any analytical work. In these instances, the CAU sent requesters a

---

[56] In response to our first NSL report, the FBI OGC directed that FBI case agents ensure that, in the future, the records obtained in response to NSLs match the NSL requests. The CAU's policy now requires CAU requesters to certify to the database manager by e-mail that responsive records have been verified as accurately encompassing both the target telephone numbers and date ranges specified in the NSLs.

summary report from the database of all the data related to a particular telephone number.

C. Community of Interest/Calling Circle [redacted]

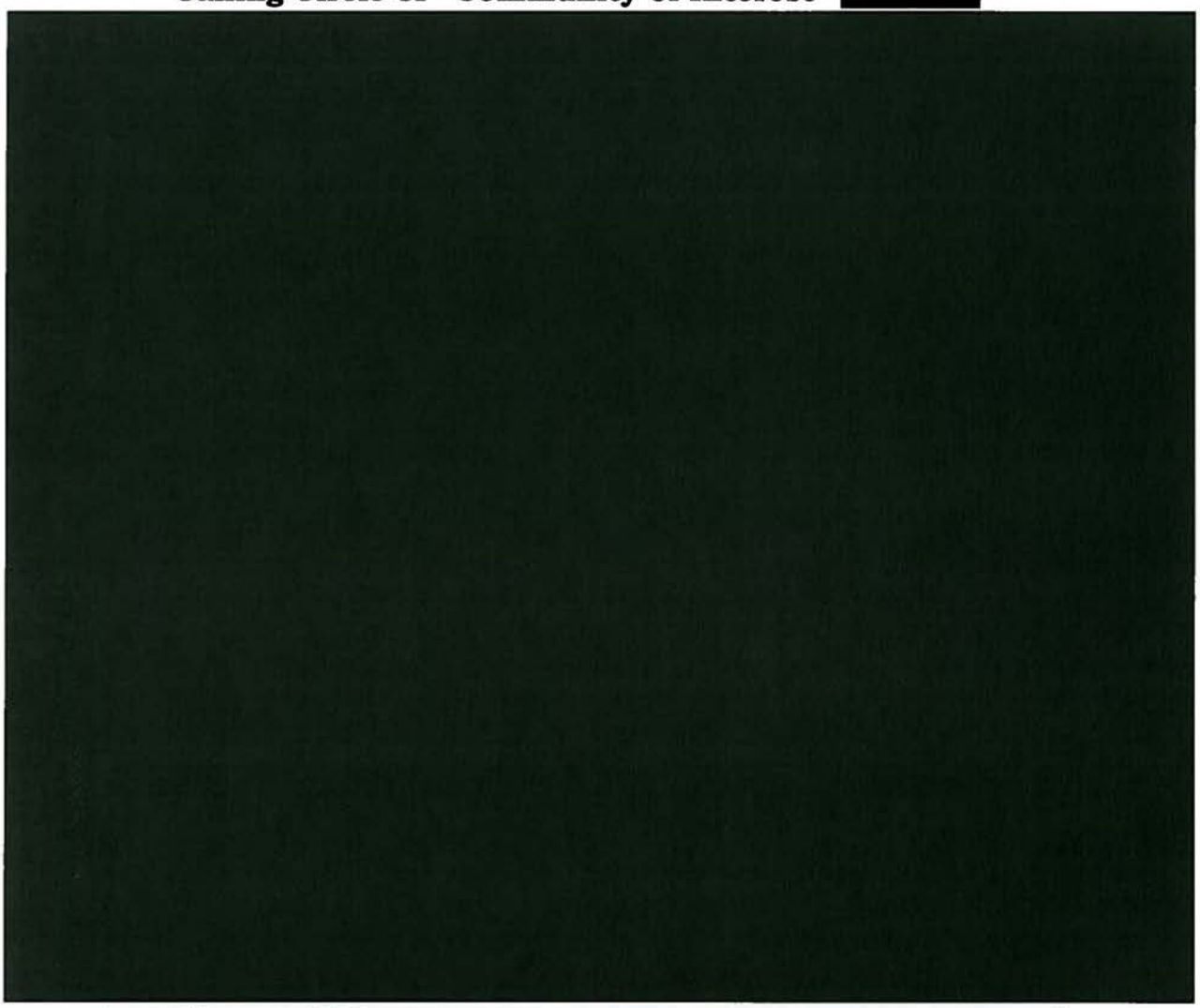
In addition, we found that the FBI often asked Company A's on-site employees [redacted] what were termed "community of interest" or "calling circle" [redacted] These requests were conveyed to Company A in NSLs, grand jury subpoenas, exigent letters, and e-mails. We determined that as part of its [redacted] contract with the FBI, on-site Company A analysts used Company A's community of interest [redacted] on records that were not identified in FBI requests. However, the FBI did not maintain documentation of how often these community of interest requests were made, and we could not determine how often the FBI acquired records in response to these [redacted]

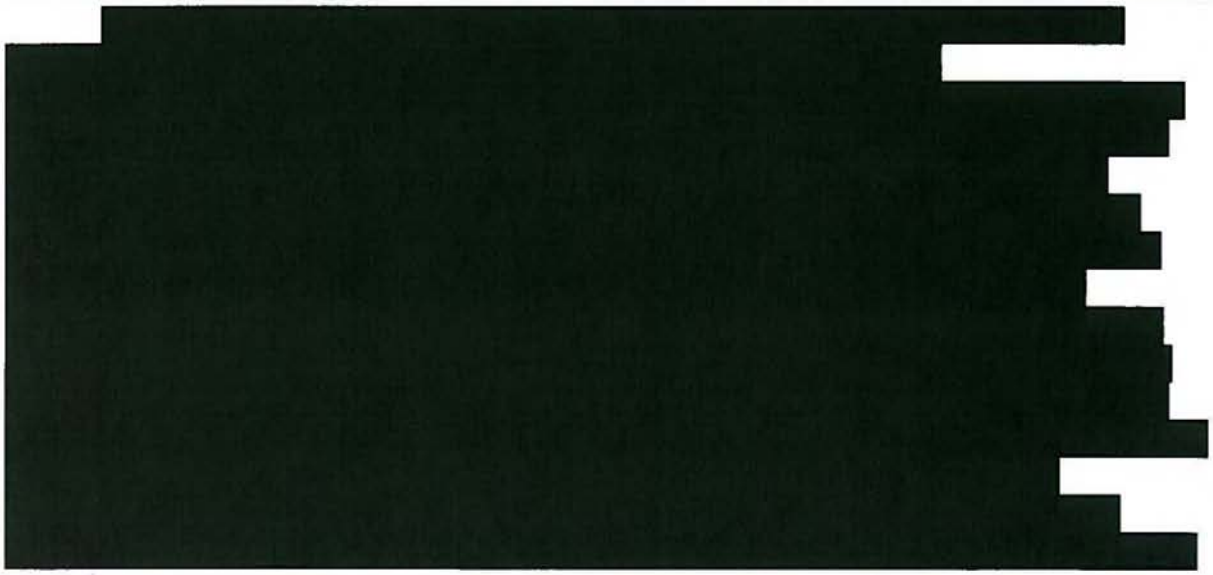
1. Community of Interest [redacted]

[redacted]

DIAGRAM 2.1

Calling Circle or "Community of Interest" [redacted]





2. Community of Interest [redacted] for the FBI

We found that FBI requests for records often included requests for community of interest [redacted] We identified 52 exigent letters (of the 514 signed by CAU personnel) served on the on-site Company A analysts that included requests for community of interest [redacted][57] We also identified more than 250 NSLs and over 350 grand jury subpoenas served on the 3 on-site providers that requested community of interest [redacted]

Prior to mid-May 2006, the FBI issued to the 3 on-site providers 107 NSLs that included in the body of the letters community of interest requests. After May 2006, the community of interest requests appeared in "boilerplate" attachments appended to over 150 NSLs. The standard attachment listed 18 types of records, including a "'calling circle' . . . based

---

[57] Even though Company B and Company C did not [redacted] community of interest [redacted], we identified 25 exigent letters to Company B and 20 exigent letters to Company C that requested such [redacted]

on a [redacted] community of interest" that the attachment stated "may be considered by you to be toll billing records pursuant to § 2709." The FBI Assistant General Counsel had drafted this attachment for the CAU. It was retained on the CAU's share drive and accessible by all CAU personnel and the on-site providers.[58]

We determined that community of interest [redacted] generally were [redacted] after the Company A analyst confirmed with CAU personnel that such a [redacted] was needed. In addition, in some instances, prior to [redacted] such [redacted], CAU personnel asked that the community of interest [redacted] In other instances, the [redacted][59] Thus, it appears that community of interest [redacted] requests often were included as boilerplate language in NSLs served on the on-site Company A analysts, although Company A did not necessarily [redacted] such [redacted] in each instance.

We found evidence that some FBI officials who signed NSLs that contained community of interest [redacted] requests were not even aware that they were making such requests. For example, NSLB Deputy General Counsel Julie Thomas, who signed at least four NSLs dated from February 2005 to August 2005 requesting in the body of the letters community of interest [redacted], told us that she was not aware of Company A's community of interest capability until June 2006, when Company A representatives briefed her and other FBI OGC attorneys on Company A's capabilities under its contract with the FBI. Thomas said that if she had signed NSLs prior to June 2006 containing a community of interest [redacted] request, the request would "probably not" have meant anything to her

---

[58] This NSL attachment was similar to a model standard NSL attachment the FBI's National Security Law Branch (NSLB) in FBI OGC had previously circulated to FBI personnel and posted on its Intranet website. The previous standard NSL attachment listed all of the records identified in the post-May 2006 attachment except calling circle records.

[59] We reviewed exigent letters and NSLs that contained the following text: "In addition, please provide a 'calling circle' for the foregoing telephone number(s) [redacted]

because she had not yet had the briefing from Company A.[60] The approval ECs we obtained that accompanied these NSLs did not mention community of interest [redacted] or [redacted] records.

Similarly, two NSLs signed by then Acting CTD Deputy Assistant Director Arthur Cummings III in October 2006 and an NSL signed by then CTD Assistant Director Joseph Billy, Jr., in January 2006 contained community of interest [redacted] requests, although the corresponding approval ECs did not address that community of interest [redacted] were to be [redacted] or the predication for these [redacted] requests under the ECPA.[61] Thomas told us that there "appears to be the strong potential" that other FBI personnel made community of interest [redacted] requests without "understanding what it means" and that "the appropriate relevance inquiry is not being done."

We requested the approval ECs for 28 NSLs issued between July 28, 2004, and May 2, 2006, to the 3 on-site providers that included requests for community of interest records in the body of the NSLs. The FBI located approval ECs for only 21 of these NSLs. Of these 21 approval ECs, only 4 stated that community of interest records were being requested and only 2 described the relevance of [redacted] records to the investigation.

We also requested the approval ECs for 25 NSLs issued between May 22, 2006, and December 21, 2006, to the 3 on-site providers that included standard attachments requesting community of interest records. The FBI located approval ECs for only 17 of these NSLs. Of these 17 approval ECs, none stated that community of interest records were being requested or described the relevance of [redacted] records to the investigation. This indicates that officials who signed NSLs containing community of interest requests in the letters or attachments often were unaware that they were making such requests.

Senior CTD officials we interviewed said they did not know how often community of interest [redacted] had been [redacted] by Company A. Although most CAU SSAs and Intelligence Analysts said they knew about

---

[60] In contrast, Thomas said she performed a relevancy analysis when she signed NSLs that included community of interest [redacted] requests in late 2006 in connection with a major FBI counterterrorism operation.

[61] Cummings told us that he did not understand the concept of Company A's community of interest [redacted] until after release of the OIG's first NSL report in March 2007. Billy said that he knew about Company A's community of interest [redacted] by 2004 or 2005.

Company A's ability to [redacted] community of interest [redacted], none told us that they had ever personally requested community of interest [redacted] from the on-site Company A employees.

The CAU Intelligence Analyst responsible for the team that uploaded toll billing records into the [redacted] database told us that when the responsive data was delivered to his team for uploading, the team could not distinguish [redacted] numbers provided by Company A in response to community of interest requests. He said he would only be able to identify the records derived from the community of interest requests by analyzing the information accompanying the original request and other background information. This CAU Intelligence Analyst told us that no one in the FBI had ever asked him to segregate records obtained in response to community of interest [redacted] requests or asked any questions about the practice.

Based on our review, we believe that in most instances when CAU personnel asked the on-site Company A analysts to [redacted] community of interest [redacted], Company A initially provided toll billing records for only the target numbers ([redacted] records). We found some e-mails showing that the CAU or other FBI requesters reviewed these records and identified [redacted] telephone numbers for which they requested [redacted] records. However, in responding to these requests for [redacted] records, the on-site Company A analysts did not request and the FBI did not provide separate legal process for the [redacted] records.[62] For example, we found e-mails showing that Company A analysts interpreted community of interest requests as authority to run [redacted] telephone numbers without requiring [redacted] legal process.[63] Similarly, a CAU Intelligence Analyst told us that community of interest requests "could be used to obtain the [redacted] [toll records] without a new NSL or grand jury subpoena."

---

[62] [redacted]

[63] In a September 2006 e-mail to CAU personnel, an on-site Company A analyst wrote that "the [community of interest] language in the [attachment] will allow [Company A] to provide call detail records without [redacted] authority."

Thus, while the NSLs containing the community of interest [redacted] request language were signed by FBI officials who were delegated the authority to sign NSLs, the actual decisions about which [redacted] records were [redacted] were made by CAU Intelligence Analysts, Supervisory Special Agents, and Special Agents who were not among those to whom the FBI Director delegated authority to sign NSLs.[64] As a result, in cases where the NSL signer was unaware that the NSL or attachment contained a community of interest request, the decisions to [redacted] the [redacted] records were made without the appropriate official having made the determination required by the ECPA that the [redacted] telephone numbers were relevant to authorized national security investigations.

As we describe in the analysis at the end of this chapter, if the FBI was able to establish before issuing the NSL that the [redacted] telephone numbers were relevant to an authorized national security investigation, we believe a separate NSL for the [redacted] telephone numbers was not required before requesting or obtaining records on the [redacted] telephone numbers. However, if the FBI did not establish the relevance of the [redacted] telephone numbers prior to the initial [redacted], reliance on the original NSL to obtain [redacted] telephone records violated the ECPA, the Attorney General's NSI Guidelines, and FBI policy.

NSLB attorneys told us that prior to the FBI's implementation of an automated system to facilitate the issuance of NSLs and collection of data on NSL usage for required reports to Congress, the FBI had not determined whether it had acquired any [redacted] records on U.S. persons that should have been reported to Congress.[65] The FBI's automated NSL system

---

[64] Prior to the Patriot Act, approximately 10 FBI Headquarters officials were authorized to sign national security letters, including the FBI Director, Deputy Director, and the Assistant Directors and Deputy Assistant Directors of the Counterterrorism and Counterintelligence Divisions. However, the Patriot Act also authorized the heads of the FBI's 56 field offices (Assistant Directors in Charge or Special Agents in Charge) to issue NSLs. Since enactment of the Patriot Act, approval to sign NSLs has been delegated to the Deputy Director, Executive Assistant Director (EAD), and Assistant EAD for the National Security Branch; Assistant Directors and all Deputy Assistant Directors for the Counterterrorism, Counterintelligence, and Cyber Divisions; all Special Agents in Charge of the New York, Washington, D.C., and Los Angeles field offices, which are headed by Assistant Directors in Charge; the General Counsel; and the Deputy General Counsel for the National Security Law Branch in the Office of the General Counsel.

[65] The FBI's new NSL "subsystem" for creating NSLs is described in the OIG's second NSL report. OIG, NSL II, 21.

implemented in January 2008 requires the user to enter the total number of telephone numbers for which toll billing records are requested in each NSL.[66]

3. Company A's Use of Community of Interest [redacted]

Based on information provided by the on-site Company A analysts and other information from Company A, we found that Company A's on-site analysts used the community of interest [redacted] services Company A provided to the FBI. One Company A analyst estimated he may have used the community of interest [redacted] for up to 25 percent of the [redacted] he [redacted] Company A records show that from 2004 to 2007, Company A analysts used its community of interest [redacted] to review records in its database for 10,070 [redacted] telephone numbers. We believe that most of these numbers were [redacted] by Company A analysts without community of interest requests from the FBI but did not generate records that were provided to the FBI. A Company A attorney told us, based on information provided to him, that the majority of the community of interest [redacted] by the on-site Company A analysts did not result in disclosure of any data to the FBI. However, we found that Company A did not request and the FBI did not provide legal process or exigent letters in connection with Company A's use of its community of interest [redacted] as part of its [redacted] support services.

[redacted]

[66] After reviewing a draft of this report, FBI officials told us that they expect to add a feature to the automated system to capture data on [redacted] numbers.

[redacted]

4. FBI Guidance on Community of Interest [redacted] Requests

Glenn Rogers, who was the CAU's first permanent Unit Chief beginning in March 2003, told us that the NSLB had approved the use of community of interest [redacted], although he said he could not recall the name of the NSLB attorney who had approved their use. Bassem Youssef, who succeeded Rogers as the CAU Unit Chief in November 2004, told us that he was present at a June 2006 briefing by Company A representatives for FBI OGC attorneys and DOJ personnel on Company A's capabilities, which included a reference to the community of interest [redacted] Youssef said that no one in the FBI OGC raised any questions about community of interest [redacted] at the time and that he never heard from FBI OGC attorneys about the issue until it was raised during the OIG's first NSL review.

We determined that in November 2004 and December 2004, the NSLB Assistant General Counsel first exchanged e-mails with several CAU employees regarding the use of language such as "a 'calling circle' based on a [redacted] community of interest" in the body of NSLs or the accompanying attachments to NSLs.[67] After reviewing the language used in the CAU's community of interest requests, the Assistant General Counsel expressed concern to a CAU SSA that the [redacted] information may be "running a little far a field." The Assistant General Counsel thereafter checked with then NSLB Senior Counsel for National Security Affairs Marion Bowman about the CAU's practice of obtaining [redacted] telephone records using NSLs. Bowman replied that he thought the FBI's acquisition of records on [redacted] numbers was authorized if the records "related" to an investigation, but stated that [redacted] records [redacted] Thereafter, by e-mail dated March 7, 2005, the Assistant General Counsel told Rogers and Youssef that NSLB could "make an argument" that [redacted] records are relevant, but that [redacted] records would require additional information supporting the position that the records were relevant.

---

[67] Although the first e-mail exchanges we found on this topic were in November 2004, we found that community of interest [redacted] requests were contained in exigent letters, grand jury subpoenas, and NSLs as early as February 2003.

While no formal legal review of community of interest [redacted] was undertaken by the FBI, the Assistant General Counsel stated that, "we had generally allowed the CAU to do it because, as we understood it, their cases are often more serious and involve immediate threats." However, she said she believed the community of interest feature was used by the CAU only in urgent circumstances "where you don't have time to do an investigation kind of piece by piece." The Assistant General Counsel stated, "The only reason you do a [redacted] in the very beginning is because you don't really have the time and you think the situation is serious enough that you need to get that information right away." She explained that NSLB had approved the community of interest attachment for NSLs served on the on-site providers based on a relevancy analysis that took into account the immediacy and seriousness of the underlying threats for which the CAU provided operational support, rather than on a relevancy analysis of the [redacted] telephone numbers that would [redacted]

FBI General Counsel Caproni and NSLB Deputy General Counsel Thomas told us that while the FBI has not issued written guidance on community of interest [redacted] requests, they concluded based on their own legal analysis that community of interest [redacted] records could satisfy the ECPA relevance standard. Caproni stated that the ECPA relevance requirement does not necessarily mean that only [redacted] records are relevant to an investigation. Thomas also stated that any relevance assessment of the [redacted] telephone numbers would be "very fact specific" and that, based on the nature of the [redacted] target, the [redacted] records could be relevant under the ECPA.

In March 2007, after the OIG raised questions about community of interest [redacted] requests in connection with our ongoing exigent letters investigation, the FBI directed its employees [redacted] In April 2007, the Assistant General Counsel instructed all Chief Division Counsels (CDC) in FBI field divisions to contact NSLB if they saw any community of interest requests.[68]

---

[68] CDCs in all 56 FBI field divisions report to the Special Agents in Charge of the field division and are responsible for reviewing all NSLs prepared for the signature of the Special Agent in Charge. The Assistant General Counsel stated in her April 9, 2007, e-mail to the CDCs that NSLB had "opined to CAU that in certain situations, they can ask for and obtain from the embedded carriers information on a [redacted] of calls, i.e., [redacted] She stated that such requests must be made in the NSL attachment (which lists the type of information the provider "may consider to be 'toll billing records'," not the body (Cont'd.)

Beginning in May 2007, several draft policies on community of interest [redacted] requests were circulated between the CTD and the FBI OGC. The latest draft dated November 23, 2007, addressed circumstances in which community of interest [redacted] would be authorized using NSLs or subpoenas. The draft policy stated that [redacted]

On December 16, 2008, the FBI issued the FBI's Domestic Investigations and Operations Guide (DIOG), which provides specific guidance for requesting community of interest records. The DIOG requires that NSLs requesting community of interest records must be approved by the NSLB Deputy General Counsel and served on the CAU, and that [redacted] telephone numbers for which information is obtained must be reported to the NSLB for congressional reporting purposes.[69]

The DIOG further provides that "if an NSL is seeking [redacted] records, the NSL [approval] EC must clearly state that [redacted] information is being sought and must demonstrate the relevance of the [redacted] information to the national security investigation."[70] We agree with this requirement and concluded that in order to satisfy the ECPA this relevance assessment must be made before issuance of NSLs seeking [redacted] records.

VI. OIG Analysis

A. Requests for Telephone Records through Exigent Letters and Other Informal Requests

To protect the confidentiality of telephone and e-mail subscriber information and telephone toll billing records information, the ECPA states that wire or electronic communications service providers "shall not

---

of the NSL, and that the attachment required legal sign-off on the relevancy of the information sought to the investigation.

[69] Federal Bureau of Investigation, Domestic Investigations and Operations Guide (FBI DIOG), §§ 11.9.3(E) & (E)(3).

[70] FBI DIOG, § 11.9.3(E)(3).

knowingly divulge a record or other information pertaining to a subscriber or customer of such service . . . to any government entity."[71] The ECPA NSL statute contains an exception to the confidentiality of such records by requiring communications service providers to provide covered records to the FBI if the FBI Director or his designee certifies in writing that the records sought are

> 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 upon the basis of activities protected by the first amendment to the constitution of the United States.[72]

During the period covered by our review, the Attorney General's NSI Guidelines authorized the use of NSLs only during investigations of international terrorism or espionage, upon the signature of a Special Agent in Charge or other designated senior FBI official.[73] In order to open such investigations, the FBI must satisfy certain evidentiary thresholds, which must be documented in FBI case files and approved by supervisors.[74] If case agents want to issue NSLs, FBI policies require a 4-step approval process. Case agents must secure the approval of their supervisors, the Chief Division Counsel, an Assistant Special Agent in Charge, and the Special Agent in Charge (or equivalent supervisors and attorneys at FBI Headquarters), who signs the NSL.

We concluded in our first NSL report that the CAU's use of exigent letters was a circumvention of the ECPA NSL statute.[75] We found that neither the ECPA, the Attorney General's NSI Guidelines, nor FBI policy authorize the FBI to obtain ECPA-protected records by serving this type of informal letter prior to obtaining the records, with "legal process to follow." In limited circumstances a separate provision of the ECPA authorizes the FBI to obtain non-content telephone records from communications service

---

[71] 18 U.S.C. § 2702(a)(3).

[72] 18 U.S.C. §§ 2709(a) and 2709(c).

[73] The Attorney General's NSI Guidelines were replaced by a new set of Attorney General Guidelines, the Attorney General Guidelines for Domestic Operations, which became effective on December 1, 2008. The new guidelines do not alter the requirement for NSLs issued in national security investigations.

[74] OIG, NSL I, 17-18.

[75] OIG, NSL I, 95-98.

providers. During 2003 through March 8, 2006 – the period when most of the exigent letters were issued – that provision authorized a provider to voluntarily release toll records information to a governmental entity if the provider "reasonably believe[d] that an emergency involving immediate danger of death or serious physical injury to any person justifie[d] disclosure of the information."[76] However, we did not agree with the FBI's after-the-fact rationale that the letters could be justified under this provision for several reasons, including that the letters were sometimes used in non-emergency circumstances and that senior CAU officials and FBI attorneys told us they did not rely on the emergency voluntary disclosure provision to authorize the exigent letters at the time.[77] We discuss the potential application of the emergency voluntary disclosure provision to exigent letters and other informal requests in greater detail in Chapter Six.

In this review, we found that many FBI supervisors and employees issued or approved these exigent letters even though the letters on their face contained statements that were inaccurate, such as that a grand jury subpoena had already been submitted to the U.S. Attorney's Office and would be served as expeditiously as possible. Yet, when we asked these FBI supervisors and employees why they issued such letters stating that subpoenas were forthcoming, no one could satisfactorily explain their actions. Instead, they gave a variety of unpersuasive excuses, contending either that they thought someone else had reviewed or approved the letters, or that they had inherited the practice and were not in a position to change it, or that the communications service provider accepted the letters. But with few exceptions, no one objected to the inaccurate statements in the letter. Moreover, we found instances in which the signers of exigent letters did not know whether there were exigent circumstances.

In Chapter Five of this report, we assess the accountability of individual FBI supervisors and employees for these improper practices. However, we believe it is important to note here the widespread failure to object to letters that contained inaccurate statements on their face. For FBI officials and employees to unquestioningly issue hundreds of these improper

---

[76] 18 U.S.C. § 2702(c)(4) (Supp. 2002). In March 2006, the provision was amended by the *PATRIOT Improvement and Reauthorization Act of 2005* to allow voluntary disclosure "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency." *USA PATRIOT Improvement and Reauthorization Act of 2005*, Pub. L. No. 109-177, § 119(a), 120 Stat. 192 (2006).

[77] OIG, NSL I, 96-97.