

and improved the handling of Stellar Wind-related discovery issues in international terrorism prosecutions. ~~(TS//STLW//SI//OC/NF)~~

Second, we do not believe that reading in a few additional Department attorneys during the first 2 years of the program would have jeopardized national security as suggested by Gonzales, especially given the hundreds of operational personnel who were cleared into the program during the same period (see Chart 4.1). In fact, as noted above, we think the highly classified nature of the program, rather than constituting an argument for limiting the OLC read-ins to a single attorney, made the need for careful analysis and review within the Department and by the NSA only more compelling.

~~(TS//SI//NF)~~

In sum, we concluded that the departure from established OLC and Department practices resulted in legal opinions to support the program that were later determined to be flawed. We believe the strict control over the Department's access to the program undermined the role of the Department to ensure the legality of Executive Branch actions, and as discussed below, contributed to the March 2004 crisis that nearly resulted in the mass resignation of the Department's leadership. ~~(TS//SI//NF)~~

We recommend that when the Justice Department is involved with such programs in the future, the Attorney General should carefully assess whether the Department has been given adequate resources to carry out its vital function as legal advisor to the President and should aggressively seek additional resources if they are found to be insufficient. We also believe that the White House should allow the Department a sufficient number of read-ins when requested, consistent with national security considerations, to ensure that sensitive programs receive a full and careful legal review. (U)

#### **B. The Hospital Visit (U)**

The Department's reassessment of Yoo's analysis led Comey, who was exercising the powers of the Attorney General while Ashcroft was hospitalized in March 2004, to conclude that he could not certify the legality of the Stellar Wind program. In response, the President sent Gonzales and Chief of Staff Andrew Card to visit Ashcroft in the hospital to seek his certification of the program, an action Ashcroft refused to take. We believe that the way the White House handled its dispute with the Department about the program – particularly in dispatching Gonzales and Card to Ashcroft's hospital room to override Comey's decision – was troubling for several reasons. ~~(TS//SI//NF)~~

As discussed in this chapter, by March 2004, when the Presidential Authorization was set to expire again, Goldsmith had placed Gonzales and Addington on notice for several months of the Department's doubts about

the legality of aspects of the Stellar Wind program. In particular, he and Philbin had made clear that the Department questioned the legality of the collections of [REDACTED].<sup>230</sup>

~~(TS//STLW//SI//OC/NF)~~

After Attorney General Ashcroft was hospitalized and unable to fulfill his duties, the White House was informed that Deputy Attorney General Comey had assumed the Attorney General's responsibilities. We found that the assertion by some in the White House at the time that they had not been informed of the situation was subsequently contradicted by the facts. In particular, Gonzales later acknowledged that he was aware that Comey was acting as the Attorney General.<sup>231</sup> (U)

Before the Presidential Authorization was set to expire on March 11, Comey, who was exercising the powers of the Attorney General at the time, told top officials in the White House – including Vice President Cheney and White House Counsel Gonzales – that the Justice Department could not recertify the legality of the program as it was presently operating. The White House disagreed with the Justice Department's position, and on March 10, 2004, convened a meeting of eight congressional leaders to brief them on the Justice Department's seemingly sudden reluctance to recertify the program and on the need to continue the program. The White House did not invite anyone from the Department to this briefing to describe the basis for its advice about the legality of the program, nor did it inform the Department of its intention to hold the meeting.<sup>232</sup> ~~(TS//SI//NF)~~

Following this briefing, Gonzales and Card went to the hospital to ask Attorney General Ashcroft, who was in the intensive care unit recovering

---

<sup>230</sup> Our conclusion that Goldsmith advised Gonzales and Addington of the Department's concerns in December 2003 is supported by his contemporaneous notes of these events. In addition, although Gonzales told us that the first time he recalled hearing of these concerns in detail was in early March 2004, he did not dispute that Goldsmith had first begun to advise him of the Department's general concerns months earlier. (U)

<sup>231</sup> During his congressional testimony, when questioned about whether he knew that Attorney General Ashcroft's powers had been transferred to Comey, Gonzales responded, "I think that there were newspaper accounts, and that fact that Mr. Comey was the acting Attorney General is probably something I knew of." (U)

<sup>232</sup> On the advice of White House counsel, Gonzales declined to provide a reason to the OIG why the Department was not asked to participate in the briefing. However, when Gonzales commented on a draft of this report, he stated that the purpose of the meeting was to inform the congressional leaders that the Department had a problem with the legal basis for aspects of the program, [REDACTED] and that a legislative fix therefore was necessary. Gonzales stated that the purpose of the meeting was not to have a "debate" between the White House and the Department concerning the legality of the program, but rather to explore just such a legislative "fix."

~~(TS//SI//NF)~~

from surgery and according to witnesses appeared heavily medicated, to certify the program, notwithstanding Comey's stated opposition. Yet, they did not notify Comey or anyone else in the Department that they intended to take this action. Their attempt to have Ashcroft recertify the program did not succeed. Ashcroft told them from his hospital bed that he supported the Department's legal position, but that in any event he was not the Attorney General at the time - Comey was. (U)

Gonzales stated that even if he knew that Ashcroft was aware of Comey's opposition to recertifying the program, Gonzales would still have wanted to speak with Ashcroft because he believed Ashcroft still retained the authority to certify the program. Gonzales testified before the Senate Judiciary Committee in July 2007 that although there was concern over Ashcroft's condition, "We would not have sought nor did we intend to get any approval from General Ashcroft if in fact he wasn't fully competent to make that decision." Gonzales also testified, "There's no governing legal principle that says that Mr. Ashcroft, if he decided he felt better, could decide, 'I'm feeling better and I can make this decision, and I'm going to make this decision.'" (U)

We found this explanation and the way the White House handled the dispute to be troubling. Rather, we agree with Director Mueller's observation, as recorded in his program log following his meeting with Card on March 11, 2004, that the failure to have Department of Justice representation at the congressional briefing and the attempt to have Ashcroft certify the Authorization by overruling Comey "gave the strong perception that the [White House] was trying to do an end run around the Acting [Attorney General] whom they knew to have serious concerns as to the legality of portions of the program." ~~(TS//SI//NF)~~

At a minimum, we would have expected the White House to alert Comey directly that it planned to brief the congressional leaders on the Department's position and that it intended to seek Ashcroft's approval of the program despite Comey and Goldsmith's stated legal position against continuing certain activities under the program. Instead, White House officials briefed congressional leaders and sought to have Attorney General Ashcroft recertify the program from his hospital bed without any notice to Comey or anyone else at the Department. We believe these actions gave the appearance of an "end run" around the ranking Justice Department official with whom they disagreed. ~~(TS//SI//NF)~~

**C. Recertification of the Presidential Authorization and Modification of the Program (U)**

As described in this chapter, the Department had notified Gonzales and Addington of its concerns about the legality of aspects of the program

for several months. In fact, the Department had made clear to the White House in December 2003 and more emphatically in a series of meetings in March 2004 that it believed that aspects of the program could not be legally supported in their existing form. Comey and Goldsmith were clear in their advice to the President and other White House officials. At the hospital, Ashcroft also expressed deep concern [REDACTED] and told Gonzales and Card that he supported the position of his subordinates. We believe that Ashcroft acted admirably under arduous circumstances. ~~(TS//STLW//SI//OC/NF)~~

Despite the legal concerns uniformly expressed by senior Department of Justice leaders, the White House, through White House Counsel Gonzales, recertified the Authorization, allowing the program to continue substantively unchanged. ~~(TS//SI//NF)~~

Only after Mueller, Comey, and other senior Department and FBI officials made known their intent to resign if the White House continued the program unchanged, despite the Department's conclusion that aspects of the program could not be legally supported, did the President direct that the issue be resolved, and the program be modified to address the Department's legal concerns. Because we were unable to interview key White House officials, we could not determine for certain what caused the White House to change its position and modify the program, although the prospect of mass resignations at the Department and the FBI appears to have been a significant factor in this decision.<sup>233</sup> According to Comey, the President raised a concern that he was hearing about these problems at the last minute, and the President thought it was not fair that he was not told earlier about the Department's legal position. In fact, as Comey informed the President, the President's staff had been advised of these issues "for weeks." ~~(TS//SI//NF)~~

Finally, we believe that the Department and FBI officials who resisted the pressure to recertify the Stellar Wind program because of their belief that aspects of the program were not legally supportable acted courageously and at significant professional risk. We believe that this action by Department and FBI officials – particularly Ashcroft, Comey, Mueller,

---

<sup>233</sup> For instance, we found it significant that on March 16, 2004, White House Counsel Gonzales, who had to make a recommendation to the President about how to proceed with the program in view of the Department's conclusion that legal support for [REDACTED] called Director Mueller to ask him whether he would resign if the President did not [REDACTED] Mueller responded that he "would have to give it serious consideration if the President decided to go ahead in the face of DOJ's finding." [REDACTED]

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

Goldsmith, Philbin, and Baker – was in accord with the highest professional standards of the Justice Department. ~~(TS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS/SI//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS/SI//ORCON/NOFORN~~

**CHAPTER FIVE**  
**STELLAR WIND PROGRAM'S TRANSITION TO FISA**  
**AUTHORITY**  
**(JUNE 2004 THROUGH AUGUST 2007)**

In this chapter we examine the transition in stages of the Stellar Wind program from presidential authority to FISA authority. We first describe the FISA Court's approval in July 2004 of the government's application to acquire foreign intelligence information through the collection of bulk e-mail meta data (basket 3 information). This application was based on a legal theory related to FISA's pen register and trap and trace device provisions. We next discuss the government's successful May 2006 application to the FISA Court for an order to obtain bulk telephony meta data (basket 2 information) by the production of business records by certain telecommunications carriers. We then describe the government's interaction with the FISA Court to place under FISA the government's authority to intercept the content of certain communications involving both domestic and foreign telephone numbers and e-mail addresses (basket 1 information). Finally, we summarize legislation enacted in August 2007 and July 2008 to amend FISA to address, among other concerns, the difficulty the government encountered in obtaining FISA authority for content collection, as well as the government's contention that certain provisions of FISA had failed to keep pace with changes in telecommunications technology. ~~(TS//STLW//SI//OC/NF)~~

**I. E-Mail Meta Data Collection Under FISA ~~(TS//SI//NF)~~**

**A. Application and FISA Court Order (U)**

[REDACTED]

The FISA Court granted this authority on July 14, 2004

[REDACTED]

~~(TS//STLW//SI//OC/NF)~~

**1. Decision to Seek a Pen Register and Trap and Trace (PR/TT) Order from the FISA Court ~~(TS//SI//NF)~~**

[REDACTED]

[REDACTED]

Philbin told us that he encountered some opposition to the FISA approach from Counsel to the Vice President David Addington, who argued that the FISA Court was unconstitutional and questioned the need to seek its authorization for e-mail meta data collection. Philbin said that he responded that obtaining an order from the FISA Court was "ironclad safe." Baker recalled attending at least one meeting at the White House with White House Counsel Gonzales and Addington to discuss whether to seek an order from the FISA Court based on FISA's pen register and trap and trace device provisions (a PR/TT Order) and how the FISA Court should be approached to obtain such an order. Baker stated that during the meeting Addington said, "We are one bomb away from getting rid of this obnoxious Court." Baker said Addington also stressed to him that there "is a lot riding on your [Baker's] relationship with this Court." ~~(TS//STLW//SI//OC/NF)~~

In contrast, Hayden told us that he did not have any concerns about transitioning the bulk e-mail meta data collection to FISA authority and was enthusiastic about the move. Hayden stated that while he believed the President had the authority to collect the bulk meta data for the NSA to conduct meta data analysis, he believes that involving an additional branch of government in the activity provided some clarity on this subject. ~~(TS//STLW//SI//OC/NF)~~

Gonzales told us that he did not recall much about the process of filing the application with the FISA Court to obtain e-mail meta data through a PR/TT Order, but stated that there may have been individuals at the White House who expressed concern that seeking the Order from the FISA Court was not a good idea. However, Gonzales told us that he was supportive of seeking the Order [REDACTED]

[REDACTED] He stated that he relied on what the intelligence professionals told him and that he would not have supported the PR/TT application if NSA Director Hayden and others did not believe the collection under the PR/TT Order provided the coverage necessary to protect the nation [REDACTED] Gonzales

also told us that there was concern at the White House that filing the PR/TT application could lead to an unauthorized disclosure of the program.

~~(TS//STLW//SI//OC/NF)~~

## 2. Briefing for Judge Kollar-Kotelly (U)

In [REDACTED] Baker, Philbin, and Goldsmith met with Gonzales and Addington at the White House to discuss how to approach Judge Kollar-Kotelly concerning the proposed PR/TT application, and it was decided to give her a "presentation" about the application. The presentation was provided to Judge Kollar-Kotelly on [REDACTED]. Present were Attorney General Ashcroft, Central Intelligence Agency Director George Tenet, FBI Director Mueller, Hayden, Gonzales, OLC Assistant Attorney General Goldsmith, Philbin, Baker, and Director of the Terrorist Threat Integration Center (TTIC) John Brennan. According to an agenda of the briefing, and as confirmed to the OIG, the presentation was given in three parts. First, Mueller, Tenet, and Brennan described the nature of the terrorist threat facing the United States, including concerns of [REDACTED].

[REDACTED] Second, Hayden described the technical aspects of the proposed bulk e-mail meta data collection, including how the information was to be collected, archived, queried, and minimized. This portion of the presentation stressed that the NSA required the collection of meta data in bulk to maximize analytic capabilities through contact chaining [REDACTED] to identify terrorist communications.<sup>234</sup> Third, Philbin explained the government's legal argument that FISA authorized the Court to approve a broad application to collect e-mail meta data under the statute's pen register and trap and trace provisions. ~~(TS//STLW//SI//OC/NF)~~

[REDACTED]  
~~(TS//SI//NF)~~

## 3. The PR/TT Application ~~(TS//SI//NF)~~

Philbin, Baker, and at least two Office of Legal Counsel attorneys assumed primary responsibility for drafting the PR/TT application to the FISA Court and a memorandum of law in support of the application.<sup>235</sup>

<sup>234</sup> The agenda refers to the "needle in haystack" metaphor to illustrate the need for bulk collection, noting "must transform streams of hay into haystack that can later be searched." ~~(TS//SI//NF)~~

<sup>235</sup> The application package, captioned [REDACTED] consisted of the application; a proposed order authorizing the collection activity and secondary orders mandating carriers to cooperate; a declaration of NSA Director Hayden explaining the technical aspects of the

(Cont'd.)

Baker said that Judge Kollar-Kotelly was given a "read-ahead copy" of the application, since it was standard practice to give the FISA Court draft applications for review. ~~(TS//SI//NF)~~

The final application was filed [REDACTED]. A short addendum to the application filed [REDACTED] it sought authorization from the FISA Court to collect. ~~(TS//SI//NF)~~

The objective of the application was to secure authority under FISA to collect [REDACTED] bulk e-mail meta data [REDACTED] the meta data to be collected under FISA authority would be stored in a database. According to the application, queries could be run against the database to identify [REDACTED] by looking for contacts with other individuals reasonably suspected to be [REDACTED] and to reveal communications links between such operatives. The resulting analytical products would then be tipped out as leads to the FBI and other elements of the U.S. Intelligence Community to find members of [REDACTED] disrupt their activities, and prevent future terrorist attacks in the United States.<sup>236</sup> ~~(TS//STLW//SI//OC/NF)~~

The Justice Department constructed its legal argument for this novel use of pen register and trap and trace devices around traditional authorities provided under FISA. Specifically, 50 U.S.C. § 1842(a)(1) authorizes the Attorney General or other designated government attorney to apply

for an order or an extension of an order authorizing or approving the installation and use of a pen register or trap and trace device for any investigation to obtain foreign intelligence information not concerning a United States person or to protect

---

proposed e-mail meta data collection and identifying the government official seeking to use the pen register and trap and trace devices covered by the application for purposes of 50 U.S.C. § 1842(c)(1); a declaration of Director of Central Intelligence Tenet describing the threat posed by [REDACTED]; a certification from Attorney General Ashcroft stating that the information likely to be obtained from the pen register and trap and trace devices was relevant to an ongoing investigation to protect against international terrorism, as required by 50 U.S.C. § 1842(c); and a memorandum of law and fact in support of the application. ~~(TS//SI//NF)~~

<sup>236</sup> The application emphasized that Internet e-mail is one of the primary methods by which [REDACTED] communicate. The memorandum of law in support of the application stated that Internet e-mail is particularly attractive to terrorists [REDACTED]

[REDACTED] ~~(TS//SI//NF)~~

against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution which is being conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order. ~~(TS//SI//NF)~~

FISA incorporated the definitions of the terms "pen register" and "trap and trace device" from 18 U.S.C. § 3127. Thus, FISA adopted as the definition of a "pen register"

a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication. ~~(TS//SI//NF)~~

18 U.S.C. § 3127(3). FISA also adopted as the definition of a "trap and trace device"

a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication. ~~(TS//SI//NF)~~

18 U.S.C. § 3127(4).

In its application the government argued that the NSA's proposed collection of meta data met the requirements of FISA by noting that the meta data sought comported with the "dialing, routing, addressing, or signaling information" type of data described in FISA's definitions of pen registers and trap and trace devices. The government also noted that nothing in these definitions required that the "instrument" or "facility" on which the device is placed carry communications of only a single user rather than multiple users. ~~(TS//SI//NF)~~

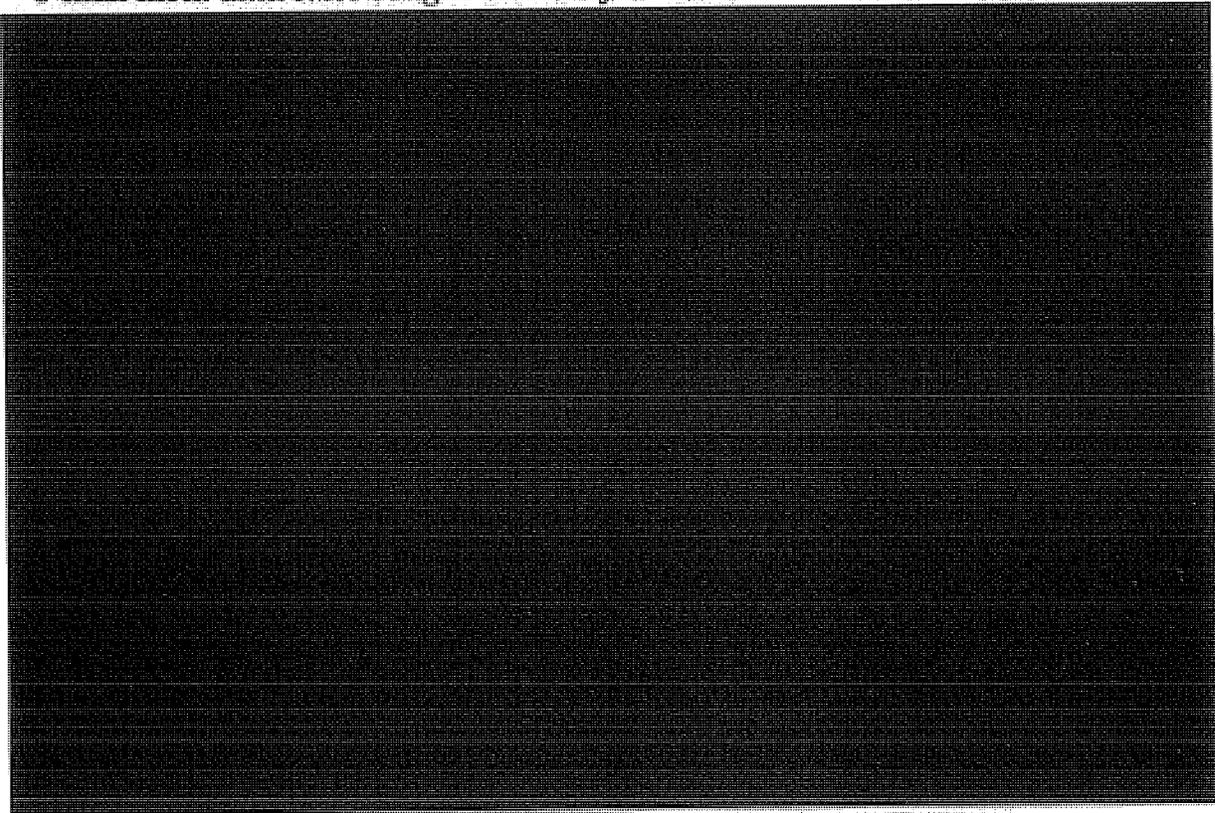
The government next argued that the information likely to be obtained from the pen register and trap and trace devices was relevant to an ongoing investigation to protect against international terrorism, as certified by the Attorney General under 50 U.S.C. § 1842(c). In support of this "certification of relevance" the government stated that the FBI was conducting more than

~~(TS//SI//NF)~~

The government acknowledged that “the overwhelming majority of communications from which meta data will be collected will not be associated with [REDACTED].” However, the government maintained that FISA did not impose any requirement to tailor collection precisely to obtain only communications that are strictly relevant to the investigation. The government argued that, in any event, “the tailoring analysis must be informed by the balance between the overwhelming national security interest at stake . . . and the minimal intrusion into privacy interests that will be implicated by collecting meta data – especially meta data that will never be seen by a human being unless a connection to a terrorist-associated e-mail is found.” ~~(TS//SI//NF)~~

The government also stated that the NSA needed to collect meta data in bulk in order to effectively use analytic tools such as contact chaining [REDACTED] that would enable the NSA to discover enemy communications. This argument echoed a premise many officials told us about the nature of intelligence gathering in general. For example, Baker likened the search for useful intelligence, particularly in the meta data context, to finding a needle in a haystack, stating, “the only way to find the needle is to have the haystack.” Gonzales argued that “to connect the dots you first have to collect the dots.” ~~(TS//SI//NF)~~

The application and supporting documents described the [REDACTED] types of e-mail meta data NSA sought authority to collect:



The application requested that the NSA be authorized to collect this meta data [REDACTED] were described as follows:

[REDACTED]

The application represented that for most of the proposed collection on [REDACTED] it was "overwhelmingly likely" that at least one end of the transmitted communication either originated in or was destined for locations outside the United States, and that in some cases both ends of the communication were entirely overseas.<sup>237</sup> However, the government acknowledged that [REDACTED]

(TS//SI//NF)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] As discussed below, the government argued and the FISA Court ultimately agreed that the above-described collection [REDACTED] [REDACTED] satisfied the definitions of pen register and trap and trace devices under FISA and Title 18. See 50 U.S.C. § 1841(2); 18 U.S.C. § 3127(3) & (4). ~~(TS//SI//NF)~~

The application also explained the proposed archiving and querying process. According to the application, the collected meta data would be stored in a secure NSA network accessible only through two administrative login accounts and by specially-cleared meta data archive system administrators. Each time the database was accessed, the retrieval request would be recorded for auditing purposes. ~~(TS//SI//NF)~~

The application proposed allowing 10 NSA analysts access to the database.<sup>238</sup> The NSA analysts were to be briefed by the NSA Office of General Counsel concerning the circumstances under which the database could be queried, and all queries would have to be approved by one of seven senior NSA officials.<sup>239</sup> ~~(TS//SI//NF)~~

The application explained that the bulk collection would be queried with particular e-mail addresses in order to conduct chaining [REDACTED]. The application proposed that queries of the e-mail meta data archive would be performed when the e-mail address met the following standard:

based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable articulable suspicion that a particular known e-mail address is associated with [REDACTED].

[REDACTED]

Under the PR/TT application, the government proposed that it be authorized under FISA [REDACTED] to use the reasonable articulable suspicion standard to query the database with specific addressing information [REDACTED].

~~(TS//STLW//SI//OC/NF)~~

In addition, the NSA proposed applying the minimization procedures in the United States Signals Intelligence Directive 18 (USSID 18) to minimize the information reported concerning U.S. persons. According to the application, compliance with these minimization procedures would be

<sup>238</sup> At the government's request the number of NSA analysts was increased to 15 when the Order was renewed [REDACTED] ~~(TS//SI//NF)~~

<sup>239</sup> When it granted the government's application, the FISA Court noted that in conventional pen register and trap and trace surveillances a court first reviews the application before a particular e-mail account can be targeted. The FISA Court stressed the importance of the NSA Office of General Counsel's obligation to ensure that the legal adequacy for such queries was met. ~~(TS//SI//NF)~~

monitored by the NSA's Inspector General and General Counsel. The government also proposed that in each renewal application the NSA would report to the FISA Court on queries that were made during the prior period and the application of the reasonable articulable suspicion standard for determining that queried addresses were terrorist-related. ~~(TS//SI//NF)~~

The application and supporting documents explained how the NSA intended to use the collected meta data. The NSA sought to use the meta data [REDACTED] to apply sophisticated algorithms to develop contact chaining [REDACTED].<sup>240</sup> In the application, the NSA estimated that through external intelligence gathering and internal analysis it would meet the proposed querying standard on average less than once a day. The NSA further estimated that these queries would generate approximately 400 tips to the FBI and CIA per year.<sup>241</sup> Of these tips to the FBI and CIA, the NSA projected that 25 percent would include U.S. person information, amounting to leads including information on about "four to five U.S. persons each month." ~~(TS//SI//NF)~~

#### 4. Judge Kollar-Kotelly Raises Questions about PR/TT Application ~~(TS//SI//NF)~~

On [REDACTED] Judge Kollar-Kotelly wrote Baker to inform him that she was considering the application and was in the process of preparing an opinion and order in response to it. She wrote that before the opinion and Order could be completed, however, she required written responses to two questions:

- (1) Apart from the First Amendment proviso in the statute (50 U.S.C. § 1842(a)(1), (c)(2)), what are the general First Amendment implications of collecting and retaining this large volume of information that is derived, in part, from the communications of U.S. persons?
- (2) For how long would the information collected under this authority continue to be of operational value to the counter-terrorism investigation(s) for which it would be collected? ~~(TS//SI//NF)~~

Baker responded in a letter to the FISA Court on [REDACTED]. Concerning the first question, Baker's letter asserted that the proposed

---

<sup>240</sup> These analytic tools are discussed in Chapter Three. (U)

<sup>241</sup> The NSA arrived at this estimate based on the assumption that each query could be expected to generate [REDACTED] e-mail addresses "one level out," and [REDACTED] addresses "two levels out." The overall number of direct and indirect contacts with the initial seed address would be significantly reduced using "analytical tradecraft." ~~(TS//SI//NF)~~

collection activity was consistent with the First Amendment and that he could find no reported decisions holding that the use of pen register and trap and trace devices violated the First Amendment. ~~(TS//SI//NF)~~

In his letter, Baker argued that although the meta data collection would include entirely innocent communications, a good-faith investigation does not violate the First Amendment simply because it is "broa[d] in scope" (quoting *Laird v. Tatum*, 408 U.S. 1, 10 (1972)). He also wrote that the use of the collected meta data would be "narrowly constrained" because the querying standard for the meta data would be subject to a "reasonable articulable suspicion" of a nexus to [REDACTED] ~~(TS//SI//NF)~~

Regarding Judge Kollar-Kotelly's second question concerning how long the collected meta data would continue to be of operational value, Baker wrote that, based on the analytic judgment of the NSA, such information would continue to be relevant to [REDACTED] for at least 18 months. Baker also advised that the NSA believed the e-mail meta data would continue to retain operational value beyond 18 months, but that it should be stored "off-line" and be accessible to queries only by a specially-cleared administrator. Baker proposed that 3 years after the 18-month timeframe, or 4½ years after it is first collected, the meta data could be destroyed.<sup>242</sup> ~~(TS//SI//NF)~~

## 5. FISA Court Order (U)

In response to the application and follow-up questions, on July 14, 2004, Judge Kollar-Kotelly signed a Pen Register and Trap and Trace Opinion and Order based on her findings that the proposed collection of e-mail meta data and the government's proposed controls over and dissemination of this information satisfied the requirements of FISA. ~~(TS//HCS//SI//NF)~~

The Order granted the government's application in all key respects. It approved for a period of 90 days the collection within the United States of e-mail meta data [REDACTED]. The Order also required the government to comply with certain additional restrictions and procedures either adapted from or not originally proposed in the application. ~~(TS//HCS//SI//NF)~~

In the Order, the Court found that the information to be collected was "dialing, routing, addressing, or signaling information" that did not include

---

<sup>242</sup> On [REDACTED] the FISA Court issued an order authorizing the NSA to maintain bulk meta data on-line for 4½ years after which time it must be destroyed. According to the NSA Office of General Counsel, the NSA still follows this retention procedure. ~~(TS//HCS//SI//NF)~~

the contents of any communication. The Court stressed that it was only authorizing collection of the [REDACTED] categories of information delineated in the application, but acknowledged that additional information "could be gleaned" from that meta data. [REDACTED]

[REDACTED] The Court found that the means by which the [REDACTED] categories of meta data were to be collected met the FISA definition of a "pen register," and that the means for collecting the [REDACTED] category of meta data satisfied the FISA definition of a "trap and trace device." See 18 U.S.C. § 3127(3) & (4), as incorporated in FISA at 50 U.S.C. § 1841(2). ~~(TS//HCS//SI//NF)~~

The Court further found that the government satisfied FISA's requirement that the application certify that the information likely to be obtained is relevant to an ongoing investigation to protect against international terrorism. The Court concluded that, "under the circumstances of this case, the applicable relevance standard does not require a statistical 'tight fit' between the volume of proposed collection and the much smaller proportion of information that will be directly relevant to [REDACTED] FBI investigations."<sup>243</sup> ~~(TS//HCS//SI//NF)~~

The Court also agreed with the government's position that the privacy interest at stake in the collection of e-mail meta data did not rise to the "stature protected by the Fourth Amendment," and that the nature of the intrusion was mitigated by the restrictions on accessing and disseminating the information, only a small percentage of which would be seen by any person. ~~(TS//HCS//SI//NF)~~

In sum, the Court concluded that the use of pen register and trap and trace devices to collect e-mail meta data would not violate the First Amendment, stating that

the bulk collection proposed in this case is analogous to suspicionless searches or seizures that have been upheld under the Fourth Amendment in that the Government's need is compelling and immediate, the intrusion on individual privacy interests is limited, and bulk collection appears to be a reasonably effective means of detecting and monitoring [REDACTED]

---

<sup>243</sup> The Court cautioned that its ruling with regard to the breadth of the meta data collection should not be construed as precedent for similar collections of the full content of communications under the electronic surveillance provisions of FISA. The Court noted important differences in the two types of collection, including the fact that overbroad electronic surveillance requires a showing of probable cause to believe the target is an agent of a foreign power, while the bulk meta data collection under FISA's pen register and trap and trace device provisions merely requires a showing that the overbroad collection is justified as necessary to discover unknown [REDACTED] persons. The Court also contrasted the high privacy interests at stake with respect to content communications with the absence of a privacy interest in meta data. ~~(TS//SI//NF)~~

[redacted] related operatives and thereby obtaining information likely to be [redacted] to ongoing FBI investigations.

~~(TS//HCS//SI//NF)~~

However, the Court also was concerned that "the extremely broad nature of this collection carries with it a heightened risk that collected information could be subject to various forms of misuse, potentially involving abridgement of First Amendment rights of innocent persons." The Court noted that under 50 U.S.C. § 1842(c)(2), pen register and trap and trace information about the communications of a U.S. person cannot be targeted for collection unless it is relevant to an investigation that is not solely based upon the First Amendment. Therefore, the Court ordered that the NSA modify its criterion for querying the archived data by inserting the following underlined language, as shown below:

[redacted] will qualify as a seed [redacted] only if NSA concludes, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable articulable suspicion that a particular known e-mail address is associated with [redacted] provided, however, that an [redacted] believed to be used by a U.S. person shall not be regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution. ~~(TS//HCS//SI//NF)~~

Regarding the storage, accessing, and disseminating of the e-mail meta data obtained by the NSA, the Court ordered that the NSA must store the information in a manner that ensures it is not commingled with other data, and must "generate a log of auditing information for each occasion when the information is accessed, to include the . . . retrieval request." The Court further ordered that the e-mail meta data "shall be accessed only through queries using the contact chaining [redacted], as described by the NSA in the government's application. ~~(TS//HCS//SI//NF)~~

The Court noted the "distinctive legal considerations" involved in implementing the authority the Court was vesting in the NSA. Specifically, the Court observed that conventional pen register and trap and trace surveillance required judicial review before any particular e-mail account could be targeted. However, by granting the government's application, the Court noted that the NSA's decision to target an e-mail address (sometimes referred to as a "seed [redacted]") would be made without judicial review. Therefore, the Court ordered that the NSA's Office of General Counsel would be responsible for training analysts to comply with querying standards and

other procedures and "to review the legal adequacy for the basis of such queries, including the First Amendment proviso . . . ." (TS//HCS//SI//NF)

As suggested by Baker in his [redacted] response to Judge Kollar-Kotelly's inquiry regarding the useful life of the collected data, the Court ordered that the e-mail meta data shall be available for 18 months for querying. The Court further ordered that after the 18-month period, the data must be transferred to an "off-line" tape system from which it could still be accessed for querying upon approval of the NSA officials authorized to approve queries, and that such meta data must be destroyed 4½ years after initially collected. (TS//HCS//SI//NF)

The Court's Order was set to expire after 90 days. The Court required that any application to renew or reinstate the authority granted in the Order must include: a report discussing queries made since the prior application and the NSA's application of the requisite legal standard to those queries; detailed information regarding [redacted] proposed to be added to the authority granted under the Order; any changes to the description of the [redacted] described in the Order or the nature of the communications [redacted]; and any changes to the proposed means of collection, including to the [redacted] of the pen register and trap and trace devices [redacted]. (TS//HCS//SI//NF)

Finally, the Court issued separate orders [redacted] to assist the NSA with the installation and use of the pen register and trap and trace devices and to maintain the secrecy of the NSA's activities. These orders [redacted] called "secondary orders," [redacted]. The NSA was directed to compensate the carriers for all assistance provided in connection with the PR/TT Order. (TS//HCS//SI//NF)

Baker and other witnesses told us that obtaining the Order was seen by the Department as a great success, and that there was general agreement that the government had secured all the authority it sought to conduct the bulk e-mail meta data collection. [redacted]

[redacted] Comey told us that obtaining the Order from the FISA Court also provided an "air of legitimacy" to the program.<sup>244</sup> (TS//STLW//SI//OC/NF)

---

<sup>244</sup> Comey and others informally referred to the PR/TT Order as "the mother of all pen registers." (TS//SI//NF)

B. **President Orders Limited Use** [REDACTED]

[REDACTED] (TS//STLW//SI//OC/NF)

E-mail meta data collection under FISA pen register authority began when the PR/TT Order took effect on July 14, 2004. As required by the Order, the data was placed in its own database or "realm." [REDACTED]

[REDACTED]

(TS//STLW//SI//OC/NF)

We discuss below the President's directive and the OLC memorandum that was drafted to analyze its legality. (TS//STLW//SI//OC/NF)

1. **The President's August 9, 2004, Memorandum to the Secretary of Defense** (TS//SI//NF)

On August 9, 2004, the same day a routine Presidential Authorization was issued to continue Stellar Wind, the President sent a separate memorandum to the Secretary of Defense regarding the use of the e-mail meta data collected [REDACTED]. The memorandum directed the Secretary of Defense that, consistent with the August 9, 2004, Presidential Authorization (and any successor Presidential Authorizations), the NSA was authorized to [REDACTED] e-mail meta data [REDACTED] when there was a reasonable articulable suspicion that (1) a party to the communication belonged to [REDACTED] and (2) the purpose of the search was to produce foreign intelligence information concerning threats [REDACTED].

<sup>245</sup> (TS//STLW//SI//OC/NF)

<sup>245</sup> The President's Memorandum provided that the authority to conduct such searches was to terminate on September 23, 2004. In the September 17, 2004, Presidential Authorization, this authority was extended until November 18, 2004. (TS//STLW//SI//OC/NF)

2. Office of Legal Counsel Determines [REDACTED]

[REDACTED]  
(TS//STLW//SI//OC/NF)

Jack Goldsmith resigned as Assistant Attorney General for the Office of Legal Counsel on July 30, 2004. Goldsmith was replaced by Daniel Levin, who served as the Acting Assistant Attorney General for OLC until February 2005. (U)

During late 2004, at the request of Comey and Ashcroft, Levin began work on an OLC memorandum addressing whether it would be lawful for the NSA to analyze the e-mail meta data collected [REDACTED]

b1, b3,  
b7E

[REDACTED]  
(TS//STLW//SI//OC/NF)

<sup>246</sup> The [REDACTED] e-mail meta data has since been placed on tape and is being held by the NSA Office of General Counsel pursuant to a preservation order.

(TS//STLW//SI//OC/NF)

<sup>247</sup> The final version of the OLC memorandum was signed by Levin on February 4, 2005. Levin told the OIG that a "policy decision" was made to limit application of the memorandum to the specific purpose [REDACTED].

However, Levin stated that, based on his analysis of the issue, he believed that [REDACTED]

(Cont'd.)

Thus, the President asserted extrajudicial authority to order the further use of e-mail meta data collected under Stellar Wind for the limited purpose described in his August 9 memorandum. The FISA Court was notified of this action, although the government did not seek its permission. ~~(TS//STLW//SI//OC/NF)~~

**C. Non-Compliance with PR/TT Order ~~(TS//SI//NF)~~**

As with other orders issued under FISA, the PR/TT Order was renewed every 90 days. During the early renewals, two major instances of non-compliance were brought to the FISA Court's attention. As described below, these violations of the Order resulted primarily from the NSA senior officials' failure to adequately communicate the technical requirements of the Order to the NSA operators tasked with implementing them, and from miscommunications among the FISA Court, the Justice Department, and the NSA concerning certain legal issues. ~~(TS//SI//NF)~~

**1. Filtering Violations ~~(TS//SI//NF)~~**

On ~~(b)(3)~~ OIPR filed a Notice of Compliance Incidents with the FISA Court. In the Notice, Baker stated that the compliance incidents cited in the Notice "raise compliance issues with about ~~(b)(3)~~ of the collection authorized by the Court."<sup>248</sup> The Notice included as an attachment a letter from NSA General Counsel Robert Deitz to Baker describing incidents that led to "unauthorized collection." Deitz learned of these incidents on ~~(b)(3)~~.<sup>249</sup> ~~(TS//SI//NF)~~

~~(b)(1), (b)(3)~~

~~(b)(1), (b)(3)~~ could be queried for any purpose. Levin told us that, other than Addington, no one else was pushing to broaden the memorandum's application. ~~(TS//STLW//SI//OC/NF)~~

<sup>248</sup> Subsequent filings indicate that ~~(b)(3)~~ of overall collections under the Order were affected by the violations. ~~(TS//SI//NF)~~

<sup>249</sup> One tipper that was based on this unauthorized collection was disseminated as a lead to the FBI but was subsequently retracted. ~~(TS//SI//NF)~~

~~(b)(1), (b)(3)~~

(Cont'd.)

(b)(1), (b)(3)

Baker told us that Judge Kollar-Kotelly was "not happy" about the violation. On (b)(3), (b)(1) the FISA Court issued an Order Regarding (b)(1), (b)(3) (Compliance Order).

The Court wrote that the "NSA violated its own proposed limitations, which were attested to by its Director and, at the government's invitation, adopted as provisions of the orders of this Court." The Court found that the violations "resulted from deliberate actions by NSA personnel," as distinguished from technical failures. The Court stated it was also troubled by the duration of the violations, which extended from July 14 through (b)(3), (b)(1) and that the Court was reluctant to issue a renewal of the PR/TT Order as to (b)(1), (b)(3) (TS//SI//NF)

That same day, the Court issued an Order to address (b)(1), (b)(3) (Order Regarding Required Information for Authorities Involving (b)(1), (b)(3)), requiring that any application for renewal or reinstatement of PR/TT surveillance authorities (b)(1), (b)(3) be accompanied by a sworn declaration by the Secretary of Defense attesting to the state of compliance with the PR/TT Order and a description of the procedures that would be used to ensure compliance. (TS//SI//NF)

On (b)(1), (b)(3) the government moved for an extension of time (until (b)(1), (b)(3)) within which to provide the Secretary of Defense's declaration. The motion, which the Court granted, assured the Court that surveillance (b)(1), (b)(3) had been terminated on (b)(1), (b)(3) and that on (b)(1), (b)(3) the NSA had moved to a separate database all meta data obtained (b)(1), (b)(3) through (b)(1), (b)(3). The NSA also represented that it reconstructed its contact chaining database using only properly obtained meta data and purged the unauthorized meta data from the system. (TS//SI//NF)

A declaration by NSA Director Hayden accompanying the government's motion stated a total of (b)(1) e-mail addresses were tipped as leads to the FBI and CIA during the violation period and that (b)(1) of these leads may have come from the unauthorized collection. Hayden wrote that

(b)(1), (b)(3)

this lead was purged from the FBI's and CIA's databases on [REDACTED]

[REDACTED] (TS//SI//NF)

The NSA Office of the Inspector General subsequently issued a report on its investigation of the unauthorized collections. The NSA OIG report stated that the filtering violations "probably led to actual unauthorized collection, but we have not been able to determine the extent of such collection, and we are not certain that we will be able to do so." The report further stated that the collection program under PR/TT Order authority was

[REDACTED] (b)(3)

[REDACTED] (TS//STLW//HCS//SI//OC/NF)

The report concluded that "there were systemic management failures within both [REDACTED] (b)(3) within the Signals Intelligence Directorate (SID)], and a complete lack of program management with regard to collection." The report stated that while the training provided by the NSA Office of General Counsel was "vigorous, conscientious, and compliant with the July 14 Order, it was inadequate in scope." (TS//STLW//HCS//SI//OC/NF)

According to the report, the NSA removed as much of the tainted collection from the PR/TT database as possible. The NSA was unable to segregate unauthorized collection from [REDACTED] (b)(1), (b)(3) so it rebuilt that portion of the PR/TT database from [REDACTED] (b)(1), (b)(3) (the day after the violation was discovered), forward. Moreover, according to the NSA OIG report, analytical personnel were restricted from accessing the unauthorized meta data. (TS//STLW//HCS//SI//OC/NF)

## 2. FISA Court Renews PR/TT Order (TS//SI//NF)

The FISA Court's PR/TT Order expired on [REDACTED] (b)(1), (b)(3) On that date the government filed its first renewal application. The Renewal Application sought authorization to collect e-mail meta data on [REDACTED] (b)(1), (b)(3) and stated that the NSA had fully complied with the PR/TT Order with respect to [REDACTED] (b)(1), (b)(3) The government did not seek reauthorization for collection [REDACTED] (b)(1), (b)(3) due to a variety of operational reasons which the application did not specify. (TS//SI//NF)

Judge Kollar-Kotelly signed the Renewal Order on [REDACTED] authorizing through [REDACTED] the use of pen register and trap and trace devices at [REDACTED] to collect e-mail meta data. The Renewal Order and the original Order were similar in most respects. However, in the Renewal Order the Court required the NSA to submit reports every 30 days concerning queries made since the prior report and describing any changes made to [REDACTED] and the [REDACTED]

<sup>251</sup> (TS//SI//NF)

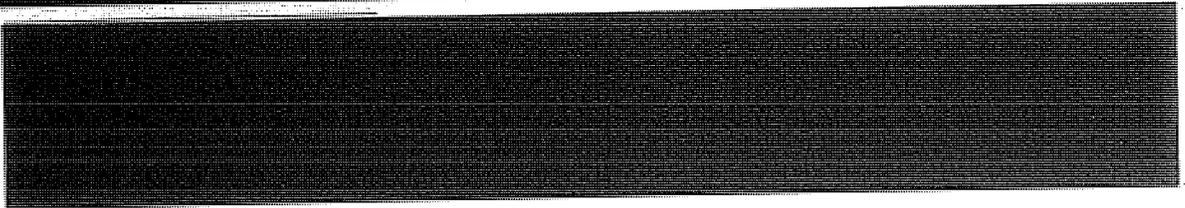
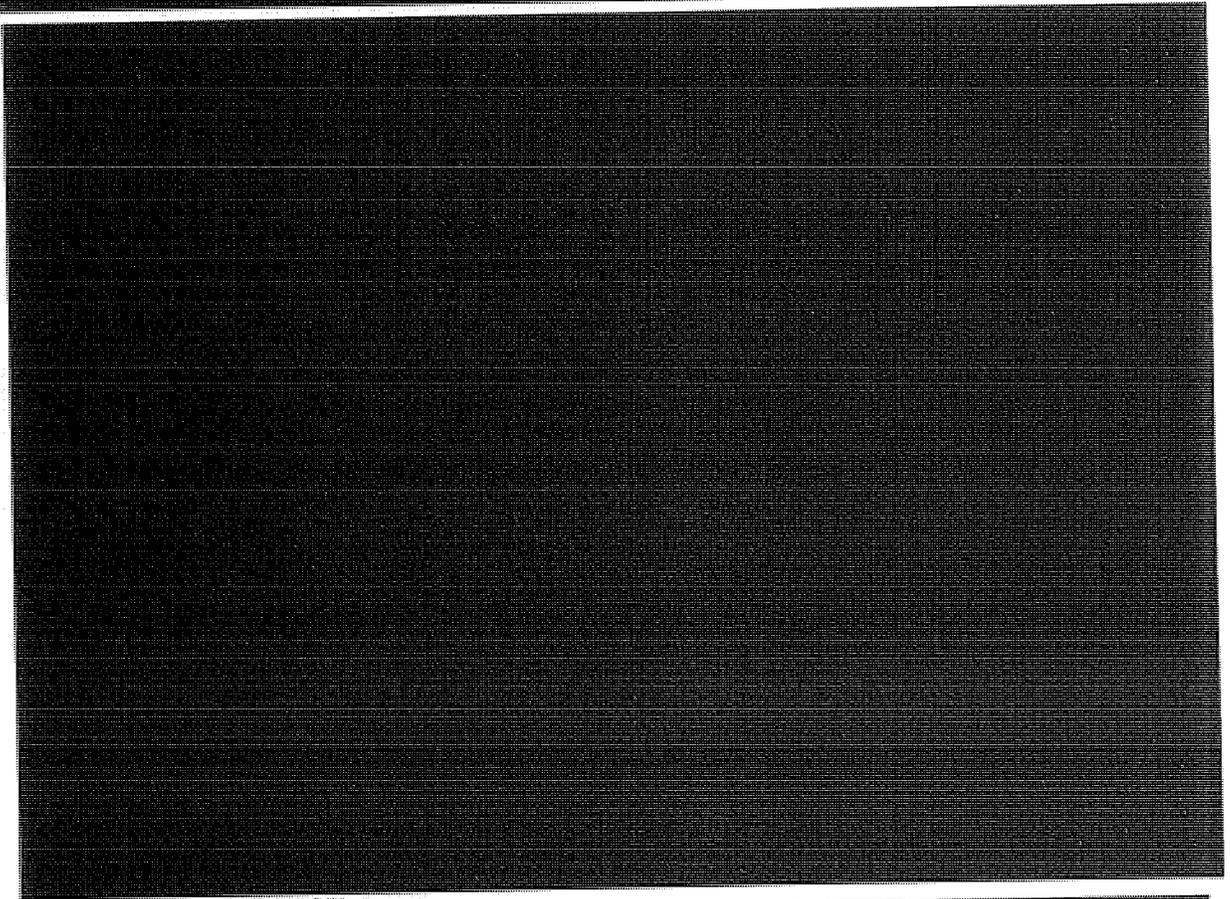
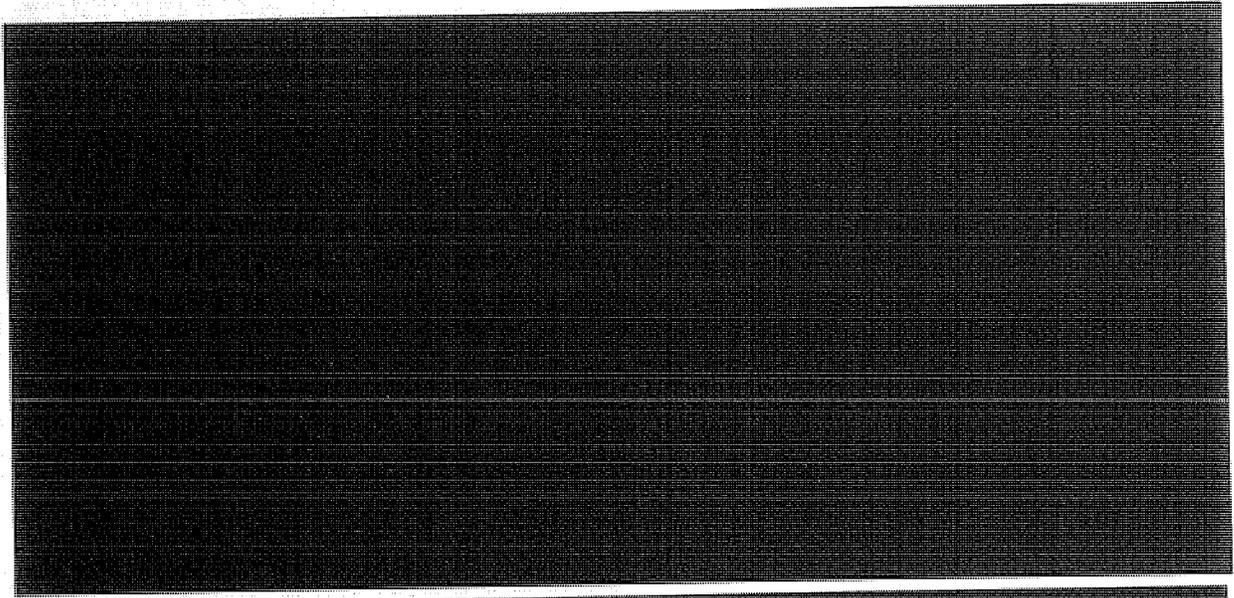
3. [REDACTED]

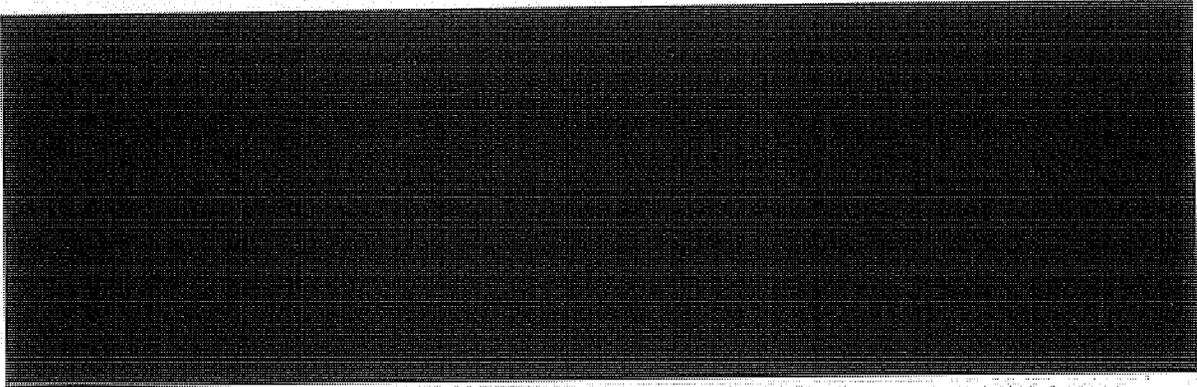
Baker told us that during one of his "oversight" visits to the NSA following the FISA Court's PR/TT Order, he was given a demonstration of how the NSA analysts processed the e-mail meta data, including an explanation of how e-mail meta data is collected and queried. Baker said he was informed that among the pieces of data that might be used to meet the reasonable articulable standard for querying the e-mail meta data [REDACTED]

(TS//STLW//SI//OC/NF)

<sup>251</sup> In the initial PR/TT Order, the Court required such a report only upon the government's submission of a renewal application every 90 days. (TS//SI//NF)

<sup>252</sup> As noted above, seed [REDACTED] are e-mail addresses or telephone numbers for which a reasonable articulable suspicion exists to believe the [REDACTED] is related to a terrorist entity. Seed [REDACTED] are used to query the meta data database to reveal links with other addresses or numbers. (TS//SI//NF)





b1,  
b3,  
b7E

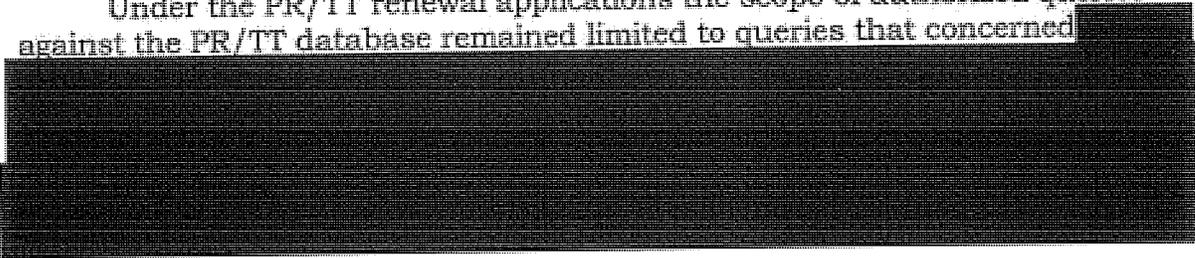
**D. Subsequent PR/TT Applications and Orders** ~~(TS//SI//NF)~~

As described above, the PR/TT Order was first renewed on [redacted] and was renewed by subsequent orders of the FISA Court at approximately 90-day intervals.<sup>254</sup> ~~(TS//SI//NF)~~

On [redacted] the FISA Court issued a Supplemental Order requiring the government to enhance its reporting to the Court of the foreign intelligence benefits realized under the PR/TT Orders. Writing for the FISA Court, Judge Kollar-Kotelly stated that the authority granted under these orders allowed the NSA "to collect vast amounts of information about e-mail [redacted] communications[,]" but that "the Court is unable on the current record to ascertain the extent to which information so collected has actually resulted in the foreign intelligence benefits originally anticipated." Supplemental Order at 1-2. The government responded with a motion requesting that, in light of prior briefings it had given the FISA Court, it not be required to fully comply with the Supplemental Order. It is not clear what if any specific action the FISA Court took in response to this motion, although based on the OIG's review of the PR/TT docket the government continued to submit regular reports to the FISA Court.

~~(TS//STLW//SI//OC/NF)~~

Under the PR/TT renewal applications the scope of authorized queries against the PR/TT database remained limited to queries that concerned [redacted]



b1,  
b3,  
b7E

<sup>254</sup> In these renewals, [redacted] were added and dropped from [redacted] that were approved in the July 14, 2004, PR/TT Order. ~~(TS//SI//NF)~~

[REDACTED]

(TS//SI//NF)

b1,  
b3,  
b7E

[REDACTED]

b1,  
b3,  
b7E

Although the FISA Court continued to renew the NSA's authority to collect and query e-mail meta data, and the NSA proceeded under that authority

[REDACTED]

b1,  
b3,  
b7E

(TS//STLW//SI//OC/NF)

**II. Telephony Meta Data Collection Under FISA (TS//SI//NF)**

The second part of the Stellar Wind program brought under FISA authority was the NSA's bulk collection of telephony meta data (basket 2). As described in Chapter Three, under this aspect of the Stellar Wind program the NSA obtained the call detail records of telephone calls domestic and international

[REDACTED]

As with e-mail meta data, the bulk

[REDACTED]

b1, b3,  
b7E

<sup>257</sup> As discussed in Chapter Three.

Call detail records consist of routing information, including the originating and terminating telephone number of each call, and the date, time, and duration of each call. The call detail records do not include the substantive content of any communication or the name, address, or financial information of a subscriber or customer. (TS//SI//NF)

nature of the telephony collection provided the NSA the ability to conduct [REDACTED] - contact chaining [REDACTED]  
(TS//STLW//SI//OC/NF) -

The transition of bulk telephony meta data collection from Presidential Authorization under the Stellar Wind program to FISA authority relied on a provision in the FISA statute that authorized the FBI to seek an order from the FISA Court compelling the production of "any tangible things" from any business, organization, or entity, provided the items are for an authorized investigation to protect against international terrorism or clandestine intelligence activities. See 50 U.S.C. § 1861. Orders under this provision commonly are referred to as "Section 215" orders in reference to Section 215 of the USA PATRIOT ACT, which amended the "business records" provision in title V of FISA.<sup>258</sup> The "tangible things" the government sought in the Section 215 application described in this section were the call detail records [REDACTED]. (TS//STLW//SI//OC/NF)

b1, b3,  
b7E

We describe below the circumstances that led to the government's decision to transition the bulk collection of telephony meta data from presidential authority to FISA Authority. We then summarize the government's initial application and the related Court Order.  
(TS//STLW//SI//OC/NF) -

**A. Decision to Seek Order Compelling Production of Call detail records (TS//SI//NF) -**

The timing of the Department's decision in May 2006 to seek a FISA Court order for the bulk collection of telephony meta data was driven primarily by external events. On December 16, 2005, The New York Times published an article entitled, "Bush Lets U.S. Spy on Callers Without Courts." The article, which we discuss in more detail in Chapter Eight, described in broad terms the content collection aspect of the Stellar Wind program, stating that the NSA had "monitored the international telephone calls of hundreds, perhaps thousands, of people inside the United States without warrants over the past three years in an effort to track possible 'dirty numbers' linked to al Qaeda." [REDACTED]

(TS//STLW//SI//OC/NF) -

<sup>258</sup> The term "USA PATRIOT Act" is an acronym for the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001). It is commonly referred to as "the Patriot Act." (U)

On December 17, 2005, in response to the article, President Bush publicly confirmed that he had authorized the NSA to intercept the international communications of people with "known links" to al Qaeda and related terrorist organizations (basket 1). On January 19, 2006, the Justice Department issued a document entitled "Legal Authorities Supporting the Activities of the National Security Agency Described by the President" and informally referred to as a "White Paper," that addressed in an unclassified form the legal basis for the collection activities that were described in the New York Times article and confirmed by the President.

~~(TS//STLW//SI//OC/NF)~~

According to Steven Bradbury, the head of OLC at that time, the legal analysis contained in the White Paper [REDACTED]

[REDACTED] Although the New York Times article did not describe this aspect of Stellar Wind, reporters at USA Today were asking about this aspect of the program in early 2006. Bradbury [REDACTED] anticipated that a USA Today story would attract significant public attention when it was published.<sup>259</sup> ~~(TS//STLW//SI//OC/NF)~~

[REDACTED]

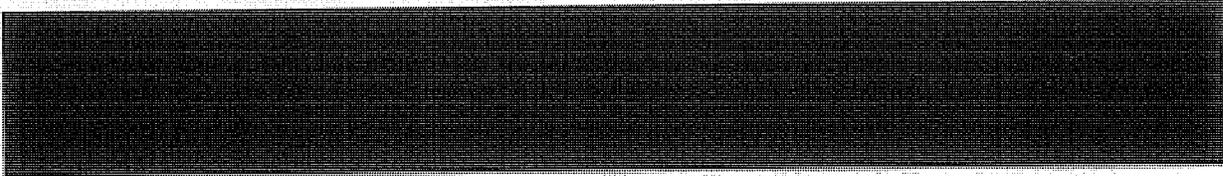
b1,  
b3,  
b7E

<sup>259</sup> On May 11, 2006, USA Today published the results of its investigation. The article, entitled "NSA Has Massive Database of American Phone Calls," reported that the NSA "had been secretly collecting the phone call records of tens of millions of Americans, using data provided by AT&T, Verizon, and BellSouth." The article stated that the program, launched shortly after the September 11 attacks, collected the records of billions of domestic calls in order to analyze calling patterns to detect terrorist activity. The article reported that the records provided to the NSA did not include customer names, street addresses, and other personal information, but noted that such information was readily available by cross-checking the telephone numbers against other databases.

~~(TS//STLW//SI//OC/NF)~~

[REDACTED]

b1,  
b3,  
b7E



**B. Summary of Department's Application and Related FISA Court Order (S/NF)**

As noted previously, applications to the FISA Court that seek an order compelling the production of "tangible things" are commonly referred to as "Section 215" applications, in reference to Section 215 of the USA PATRIOT ACT. Section 215 authorizes the FBI to request a FISA Court order

requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution. (U)

50 U.S.C. § 1861(a)(1).<sup>261</sup> Section 215 does not require that the items sought pertain to the subject of an investigation; the government need only demonstrate that the items are relevant to an authorized investigation.<sup>262</sup> (U)

On May 23, 2006, the FBI filed with the FISA Court a Section 215 application seeking authority to collect telephony meta data to assist the NSA in finding and identifying known and unknown members or agents of [REDACTED] in support of the [REDACTED] related FBI investigations then pending and other Intelligence Community operations. The application requested an order compelling [REDACTED] to produce (for the duration of the 90-day order) call detail records relating to all telephone communications maintained by the carriers. The application described call detail records as routing information that included the

b1, b3,  
b7E

<sup>261</sup> "United States person" is defined in FISA as a citizen, legal permanent resident, or unincorporated association in which a "substantial number" of members are citizens or legal permanent residents, and corporations incorporated in the United States as long as such associations or corporations are not themselves "foreign powers." 50 U.S.C. § 1801(i)(2005). (U)

<sup>262</sup> Prior to the enactment of Section 215, the FISA statute's "business records" provisions were limited to obtaining information about a specific person or entity under investigation. Also, information could be obtained only from common carriers, public accommodation facilities, physical storage facilities, and vehicle rental facilities. (U)

originating and terminating telephone number of each call, and the date, time, and duration of each call. The application stated that telephony meta data did not include the substantive content of any communication or the name, address, or financial information of a subscriber or customer. According to the application, the majority of the telephony meta data provided to the NSA was expected to involve communications that were (1) between the United States and abroad, or (2) wholly within the United States, including local telephone calls. [REDACTED]

[REDACTED] .263 (TS//SI//NF)

The application acknowledged that the [REDACTED] collection would include records of communications of U.S. persons located within the United States who were not the subject of any FBI investigation. However, relying on the precedent established by the PR/TT Order, the application asserted that the collection was needed for the NSA to perform analysis to find known [REDACTED] and to identify unknown operatives, some of whom may be in the United States or in communication with U.S. persons. The application stated that it was not possible to determine in advance which particular piece of meta data will identify a terrorist. The application stated that obtaining such bulk data increases the NSA's ability, through contact-chaining [REDACTED] to detect and identify members of [REDACTED].<sup>264</sup> In other words, according to the application, meta data analysis is possible only if the NSA "has collected and archived a broad set of metadata that contains within it the subset of communications that can later be identified as terrorist-related."<sup>265</sup> (TS//SI//NF)

<sup>263</sup> The NSA told us that the actual average amount of telephony meta data collected per day is approximately [REDACTED] call detail records and that the figure has not reached [REDACTED] (TS//SI//NF)

<sup>264</sup> [REDACTED]

<sup>265</sup> The FISA Court had stated in its July 2004 PR/TT Order that the FISA statute's "relevance" requirement is a relatively low standard and that in evaluating whether bulk meta data is "relevant" to an investigation into [REDACTED] "deference should be given to the fully considered judgment of the executive branch in assessing and responding to national security threats and in determining the potential significance of intelligence-related information." The government cited this precedent in the Section 215 application, stating, "[j]ust as the bulk collection of e-mail meta data was relevant to FBI investigations into [REDACTED] so is the bulk collection of telephony metadata described herein." (TS//SI//NF)

The application also explained how the meta data would be used.

<sup>266</sup> The database could be queried only if the NSA determined that, "based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone number is associated with [REDACTED]

[REDACTED] the Section 215 application, like the PR/TT application and Order, added the following proviso to the query standard: "provided, however, that a telephone number believed to be used by a U.S. person shall not be regarded as associated with [REDACTED] solely on the basis of activities that are protected by the First Amendment to the Constitution." ~~(TS//SI//NF)~~

According to the application, the NSA estimated that only a tiny fraction (1 in 4 million, or 0.000025 percent) of the call detail records included in the database were expected to be analyzed. The results of any such analysis would be provided, or "tipped," to the FBI or other federal agencies (as was being done under Stellar Wind).

[REDACTED] (TS//SI//NF)

The application also proposed restrictions on access to, and the processing and dissemination of, the data collected that were essentially identical to those included in the PR/TT Order. These included the requirement that queries be approved by one of seven NSA officials or managers and that the NSA's Office of the General Counsel would review and approve proposed queries of telephone numbers reasonably believed to be used by U.S. persons.<sup>267</sup> ~~(TS//SI//NF)~~

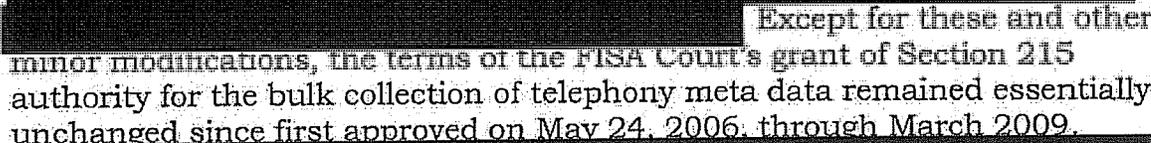
<sup>268</sup> [REDACTED]

<sup>267</sup> The application included several other measures to provide oversight of the use of meta data, such as controls on the dissemination of any U.S. person information, the creation of a capability to audit NSA analysts with access to the meta data, the destruction of collected meta data after a period of 5 years (the destruction period for e-mail meta data was 4½ years), and a review by the NSA's Inspector General and General Counsel conducted within 45 days of implementing the FISA Court order that assessed the

(Cont'd.)

On May 24, 2006, the FISA Court approved the Section 215 application. The Court's Order stated that there were reasonable grounds to believe that the telephony meta data records sought were relevant to authorized investigations being conducted by the FBI to protect against international terrorism. The Order incorporated each of the procedures proposed in the government's application relating to access to and use of the meta data. These procedures included a requirement that any application to renew or reinstate the authority for the bulk collection contain a report describing (1) the queries made since the Order was granted; (2) the manner in which the procedures relating to access and use of the meta data were applied; and (3) any proposed changes in the way in which the call detail records would be received from the communications carriers. The Order also requires the Justice Department to review, at least every 90 days, a sample of the NSA's justifications for querying the call detail records. ~~(TS//SI//NF)~~

Through March 2009, the FISA Court renewed the authorities granted in the May 24 Order at approximately 90-day intervals, with some modifications sought by the government. For example, the Court granted a motion filed on August 8, 2006, requesting

  
268  
 Except for these and other minor modifications, the terms of the FISA Court's grant of Section 215 authority for the bulk collection of telephony meta data remained essentially unchanged since first approved on May 24, 2006, through March 2009.

b1,  
b3,  
b7E

 Further, the FISA Court's Section 215 Orders did not require the NSA to modify its use of the telephony meta data from an analytical perspective. However, as discussed below, the FISA Court drastically changed the authority contained in its March 2009 Section 215 Order following the government's disclosure of incidents involving the NSA's failure to comply with the terms of the Court's prior orders.

~~(TS//STLW//SI//OC/NF)~~

---

adequacy of the management controls for the processing and dissemination of U.S. person information. ~~(TS//SI//NF)~~

<sup>268</sup> As noted above, the Court granted an identical motion at the same time in connection with the bulk collection of e-mail meta data. ~~(TS//SI//NF)~~