

C. Non-Compliance with Section 215 Orders ~~(TS//SI//NF)~~

On January 9, 2009, representatives from the Department's National Security Division attended a briefing at the NSA concerning the telephony meta data collection. During the course of this briefing, and as confirmed by the NSA in the days that followed, the Department came to understand that the NSA was querying the telephony meta data in a manner that was not authorized by the FISA Court's Section 215 Orders. Specifically, the NSA was on a daily basis automatically querying the meta data with thousands of telephone identifiers from an "alert list" that had not been determined to satisfy the reasonable articulable suspicion (RAS) standard the Court required be met before the NSA was authorized to "access the archived data" for search or analysis purposes.²⁶⁹ ~~(TS//SI//NF)~~

The alert list contained telephone identifiers that were of interest to NSA counterterrorism analysts responsible for tracking the targets of the Section 215 Orders [REDACTED]. The list was used to compare the incoming telephony meta data obtained under FISA authority. [REDACTED]

b1,
b3,
b7E

[REDACTED] Under the procedures the NSA had developed to implement the Section 215 authority, alerts (or matches) generated from RAS-approved identifiers could be used to automatically conduct contact chaining [REDACTED] of the telephony meta data. However, automated analysis for alerts generated by non-RAS approved identifiers were not permitted; instead, the alerts were sent to analysts to determine whether chaining [REDACTED] was warranted in accordance with the RAS standard. ~~(TS//SI//NF)~~

On January 15, 2009, the Justice Department notified the FISA Court that the NSA had been accessing the telephony meta data with non-RAS approved identifiers. [REDACTED]

b1, b3,
b7E

[REDACTED]²⁷⁰ On January 28, 2009, the

²⁶⁹ The term "telephone identifier" used by the government means a telephone number as well as other unique identifiers associated with a particular user or telecommunications device for purposes of billing or routing communications. ~~(TS//SI//NF)~~

²⁷⁰ Following the Department's notice to the Court, the NSA attempted to complete a software fix to the alert process so that "hits" against the telephony meta data generated by non-RAS-approved telephone identifiers were deleted and that only "hits" generated by RAS-approved identifiers were sent to NSA analysts for further analysis. The NSA also attempted to construct a new alert list consisting of only RAS-approved telephone identifiers. However, the implementation of these modifications was unsuccessful and on January 24, 2009, the NSA shut down the alert process completely. ~~(TS//SI//NF)~~

Court issued an order stating that it was "exceptionally concerned about what appears to be a flagrant violation of its Order in this matter[.]" The Court required the government to file a brief to "help the Court assess whether the Orders in this docket should be modified or rescinded; whether other remedial steps should be directed; and whether the Court should take action regarding persons responsible for any misrepresentations to the Court or violation of its Orders, either through its contempt powers or by referral to appropriate investigative offices." The Court also required the government to address several additional specific issues, including who knew that the alert list being used to query the meta data included identifiers that had not been determined to meet the reasonable and articulable suspicion standard, how long the "unauthorized querying" had been conducted, and why none of the entities the Court directed to conduct reviews of the meta data collection program identified the problem earlier.²⁷¹
(TS//SI//NF)

On February 17, 2009, the government responded to the Court's Order and acknowledged that the NSA's previous descriptions to the Court of the alert list process were inaccurate and that the Section 215 Order did not authorize the government to use the alert list in the manner that it did. The government described for the Court in detail how the NSA developed procedures in May 2006 to implement the Section 215 authority that resulted in the NSA querying the telephony meta data with non-RAS approved telephone identifiers for over 2 years in violation of the Court's Orders, and how those procedures came to be described incorrectly to the Court. According to the government, the situation resulted from the NSA's interpretation of the term "archived data" used in the Court's Orders and the NSA's mistaken belief that the alert process under the Section 215 authority operated the same as the alert process under the Pen Register/Trap and Trace authority.²⁷² The government told the Court that "there was never a complete understanding among key personnel" who reviewed the initial report to the Court describing the alert process about

²⁷¹ The entities directed to conduct such reviews under the Section 215 Orders were the NSA's Inspector General, General Counsel, and Signals Intelligence Directorate Oversight and Compliance Office. (U//FOUO)

²⁷² The NSA understood the term "archived data" in the Court's Order to refer to the NSA's analytical repository for the telephony meta data. As the term is normally used by

 The NSA believed that the requirement to satisfy the RAS standard was only triggered when the NSA sought access to the stored, or "archived," repository of telephony meta data. For this reason, in the NSA's view, it was not required to limit the alert list to RAS-approved identifiers. (TS//SI//NF)

what certain terminology was intended to mean, and that “there was no single person who had complete technical understanding of the BR FISA system architecture.” ~~(TS//SI//NF)~~

The government argued that the Section 215 Orders should not be rescinded or modified “in light of the significant steps that the Government has already taken to remedy the alert list compliance incident and its effects, the significant oversight modifications the Government is in the process of implementing, and the value of the telephony metadata collection to the Government’s national security mission[.]”²⁷³ Among the several measures the government highlighted to the Court was the NSA Director’s decision to order “end-to-end system engineering and process reviews (technical and operational) of NSA’s handling of [telephony] metadata.” Less than two weeks after the government filed the response summarized above, the government informed the Court that the NSA had identified additional compliance incidents during these reviews.²⁷⁴ ~~(TS//SI//NF)~~

In Orders dated March 2 and 5, 2009, the FISA Court addressed the compliance incidents reported by the government and imposed drastic changes to the Section 215 authorities previously granted. The Court first addressed the NSA’s interpretation of the term “archived data.” The Court said the interpretation “strains credulity” and observed that an interpretation that turns on whether the meta data being accessed has been “archived” in a particular database at the time of the access would “render compliance with the RAS requirement merely optional.” ~~(TS//SI//NF)~~

273

~~_____~~
The NSA also determined that in all instances that a U.S. telephone identifier was used to query the meta data for a report, the identifier was either already the subject of a FISA Court order or had been reviewed by the NSA’s Office of General Counsel to ensure the RAS determination was not based solely on a U.S. person’s First Amendment-protected activities. ~~(TS//SI//NF)~~

²⁷⁴ The additional compliance incidents involved the NSA’s handling of the telephony meta data in an unauthorized manner. The first incident involved the NSA’s use of an analytical tool to query (usually automatically) the meta data with non-RAS approved telephone identifiers. The tool determined if a record of a telephone identifier was present in NSA databases and, if so, provided analysts with information about the calling activity associated with that identifier. The second incident involved three analysts who conducted chaining analyses in the telephony meta data using 14 non-RAS approved identifiers. According to the government’s notice to the Court, the analysts conducted queries of non-FISA authorized telephony meta data and were unaware their queries also ran against the FISA-authorized meta data. The government stated that none of the queries used an identifier associated with a U.S. person or telephone identifier and none of the queries resulted in intelligence reporting. ~~(TS//SI//NF)~~

The Court next addressed the misrepresentations the government made to the Court from August 2006 to December 2008 in reports that inaccurately described the alert list process. The Court recounted the specific misrepresentations and summarized the government's explanation for their occurrence. The Court then concluded,

Regardless of what factors contributed to making these misrepresentations, the Court finds that the government's failure to ensure that responsible officials adequately understood the NSA's alert list process, and to accurately report its implementation to the Court, has prevented, for more than two years, both the government and the FISC from taking steps to remedy daily violations of the minimization procedures set forth in FISC orders and designed to protect ██████████ call detail records pertaining to telephone communications of U.S. persons located within the United States who are not the subject of any FBI investigations and whose call detail information could not otherwise have been legally captured in bulk. ~~(TS//SI//NF)~~

The Court also addressed the additional non-compliance incidents that were identified during the initial review ordered by the NSA Director, observing that the incidents occurred despite the NSA implementing measures specifically intended to prevent their occurrence. In view of the record of compliance incidents the government had reported to date, the Court stated,

[I]t has finally come to light that the FISC's authorizations of this vast collection program have been premised on a flawed depiction of how the NSA uses BR metadata. This misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime. The minimization procedures proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently and systemically violated that it can fairly be said that this critical element of the overall BR regime has never functioned effectively. ~~(TS//SI//NF)~~

Despite the Court's concerns with the telephony meta data program, and its lack of confidence "that the government is doing its utmost to ensure that those responsible for implementation fully comply with the Court's orders," it authorized the government to continue collecting telephony meta data under the Section 215 Orders. The Court explained that in light of the

government's repeated representations that the collection of the telephony meta data is vital to national security, taken together with the Court's prior determination that the collection properly administered conforms with the FISA statute, "it would not be prudent" to order the government to cease the bulk collection. ~~(TS//SI//NF)~~

However, believing that "more is needed to protect the privacy of U.S. person information acquired and retained" pursuant to the Section 215 Orders, the Court prohibited the government from accessing the meta data collected "until such time as the government is able to restore the Court's confidence that the government can and will comply with previously approved procedures for accessing such data."²⁷⁵ The government may, on a case-by-case basis, request authority from the Court to query the meta data to obtain foreign intelligence.²⁷⁶ Such a request must specify the telephone identifier to be used and the factual basis for the NSA's RAS determination. ~~(TS//SI//NF)~~

The Court ordered that upon completion of the NSA's end-to-end system engineering and process reviews, the government file a report that describes the results of reviews, discusses the steps taken to remedy non-compliance incidents, and proposes minimization and oversight procedures to employ should the Court authorize resumption of regular access to the telephony meta data. The government's report also must include an affidavit from the FBI Director and any other government national security official deemed appropriate describing the value of the telephony meta data to U.S. national security. ~~(TS//SI//NF)~~

Additionally, the Court ordered the government to implement oversight mechanisms proposed in the government's response to the compliance incidents. These mechanisms generally require the Justice Department's National Security Division to assume a more prominent role in the NSA's administration of the bulk collection program. For example, the NSA's Office of General Counsel must now consult with the National

²⁷⁵ The Court also stated, "Given the Executive Branch's responsibility for and expertise in determining how best to protect our national security, and in light of the scale of this bulk collection program, the Court must rely heavily on the government to monitor this program to ensure that it continues to be justified, in the view of those responsible for our national security, and that it is being implemented in a manner that protects the privacy interests of U.S. persons[.]" ~~(TS//SI//NF)~~

²⁷⁶ The Court authorized the government to query the meta data without Court approval to protect against an imminent threat to human life, with notice to the Court within the next business day of the query being conducted. The Court also authorized the government to access the meta data to ensure "data integrity" and to develop and test technological measures designed to enable to the NSA to comply with previously approved procedures for accessing the meta data. ~~(TS//SI//NF)~~

Security Division on all significant legal opinions that relate to the interpretation, scope, or implementation of past, current, and future Section 215 Orders related to the telephony bulk meta data collection.

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

On May 29, 2009, the Court authorized the government to continue collecting telephony meta data under the Section 215 Orders for 43 days subject to the same limitations set out in its orders of March 2 and 5, 2009.

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

III. Content Collection under FISA ~~(TS//SI//NF)~~

The third and last part of the Stellar Wind program brought under FISA authority was content collection (basket 1). The effort to accomplish this transition was legally and operationally complex, and our discussion in this section does not address each statutory element or the full chronology of the government's applications and related FISA Court orders. Rather, we describe the circumstances surrounding the government's decision to transition content collection from presidential to FISA authority

~~_____~~
~~_____~~
We also summarize the FISA Court's response to the government's content collection proposals and the orders it issued. In this section, we describe one FISA Court judge's rejection of the government's legal approach to content collection, a decision that hastened the enactment of legislation that significantly amended the FISA statute and provided the government surveillance authorities broader than those authorized under Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

A. Decision to Seek Content Order ~~(TS//SI//NF)~~

The Department first began work on bringing Stellar Wind's content collection activity (basket 1) under FISA in March 2005, shortly after Alberto Gonzales became Attorney General. Gonzales told us that he initiated discussions about making this change with OLC Principal Deputy Assistant Attorney General Bradbury. Gonzales said that he had questions about how the NSA was conducting the collection in terms of audits and checks being performed, and he wanted to ensure that the agency was running the program properly. Gonzales told us that placing content collection under FISA authority would also eliminate the constitutional debate about the activity and would reassure people that the President was acting according to the Constitution and the law. Gonzales said that, in his view, it is better to conduct activities such as content collection without a direct order from the President when possible. Gonzales added that in 2001 nobody thought it was possible to bring Stellar Wind under FISA authority.

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

When Gonzales became Attorney General in early 2005, however, he also knew there had been a leak to The New York Times about the NSA's content collection activity under Stellar Wind and that the paper was actively investigating the story. In November 2004, Gonzales (then the White House Counsel), together with Deputy Attorney General Comey and his Chief of Staff, had met with New York Times reporters to discuss the potential article.²⁷⁷ ~~(TS//STLW//SI//OC/NF)~~

In response to Gonzales's request, Bradbury, working with attorneys in OLC and the Office of Intelligence and Policy Review (OIPR) as well as with NSA personnel, devised a legal theory, summarized below, for bringing under FISA the Stellar Wind program's content collection activities while preserving the "speed and agility" many Intelligence Community officials cited as the chief advantage of the NSA program. In June 2005, Bradbury, together with Associate Deputy Attorney General Patrick Philbin, presented the legal theory to White House officials David Addington, Harriet Miers, and Daniel Levin and received their approval to continue work on a draft FISA application.²⁷⁸ ~~(TS//STLW//SI//OC/NF)~~

Bradbury told the OIG that he also spoke to the Director of National Intelligence and to NSA officials about bringing Stellar Wind's content collection under FISA. According to Bradbury, the Director of National Intelligence responded positively to the proposal, but the NSA was skeptical as to whether a FISA approach would be feasible, in view of the substantial administrative requirements under the FISA Court's PR/TT Order. The NSA also believed that the FISA Court would be reluctant to grant the NSA the operational flexibility it would insist on in any content application, resulting in less surveillance coverage of telephone numbers and e-mail addresses used by persons outside the United States. ~~(TS//STLW//SI//OC/NF)~~

As discussed in detail in Chapter Eight of this report, in December 2005 The New York Times published its series of articles on the content collection portion of the Stellar Wind program, resulting in considerable controversy and public criticism of the NSA program. Through the spring of 2006, the Department continued work on the content application. In May 2006, at the first of the FISA Court's semiannual meetings that year, the Department provided the Court a draft of the application for content collection to obtain feedback on the government's unconventional approach to the FISA statute. None of FISA Court judges indicated whether the

²⁷⁷ The New York Times held the article until December 2005, when it published a series of articles on the content collection portion of Stellar Wind. ~~(TS//SI//NF)~~

²⁷⁸ After serving as Acting Assistant Attorney General for OLC from June 2004 to February 2005, Levin joined the National Security Council, where he remained until approximately November 2005. (U)

application would be granted if filed, but some identified concerns with certain aspects of the proposal. ~~(TS//STLW//SI//OC/NF)~~

At this time, Congress and the Administration were also discussing how to modernize the FISA statute to authorize the type of electronic surveillance that the content application sought. Work on the application was temporarily suspended as the Department focused its attention on working with Congress to craft this legislation. However, this suspension of work on the content application was brief. Bradbury said he concluded by the fall of 2006, as Congress was heading for recess, that there would be no legislative reform of the FISA statute in the foreseeable future that would address content collection as it was being conducted under Stellar Wind. As a result, the Department pressed forward with the draft content application to the FISA Court. ~~(TS//STLW//SI//OC/NF)~~

B. Summary of Department's December 13, 2006, Content Application ~~(TS//SI//NF)~~

In November 2006, at the second of the Court's semiannual meetings, the Department presented an updated draft of the application that incorporated feedback received from members of the Court during the previous semiannual meeting. On December 13, 2006, the Department formally filed the content application with the Court. ~~(TS//SI//NF)~~

The government's December 13 application sought authority to intercept the content of telephonic and electronic communications of [REDACTED]

b1, b3,
b7E

[REDACTED] 279 The application stated:

Speed and flexibility are essential in tracking individuals who

[REDACTED] To follow the trails effectively, and to respond to new leads, it is vital for the U.S. Intelligence Community to be able quickly and efficiently to acquire communications to or from individuals reasonably believed to

279 The content application included the following caveat:

By filing this application, the United States does not in any way suggest that the President lacks constitutional or statutory authority to conduct the electronic surveillance detailed herein without Court authorization.

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

be members or agents of these [redacted] foreign powers.
~~(TS//SI//NF)~~

According to the application, the goal was to establish "an early warning system" under FISA to alert the government to the presence of members and agents of foreign powers [redacted] and to assist tracking such individuals within the United States. The "early warning system" sought to replace the conventional practice under FISA of filing individual applications each time the government had probable cause to believe that a particular phone number or e-mail address, referred to by the NSA as a "selector," was being used or about to be used by members or agents of a foreign power.
~~(TS//SI//NF)~~

b1, b3,
b7E

In the place of this individualized process, the application proposed that the FISA Court establish broad parameters for the interception of communications – specifically, [redacted] that can be targeted and the locations where the surveillance can be conducted – and that NSA officials, rather than FISA Court judges, determine within these parameters the particular selectors whose communications the NSA would intercept. [redacted] [redacted] albeit with FISA Court review and supervision.²⁸⁰ ~~(TS//SI//NF)~~

The legal arguments underlying the government's approach are complex and involve substantial communications terminology. They also require lengthy discussion of the FISA statute and previous FISA Court decisions. Rather than describe at length these issues, in this section we detail the two main components of the government's approach to content collection in the FISA application that are critical for understanding one judge's approval of the application and another judge's later rejection of essentially the same application. ~~(TS//SI//NF)~~

First, the government proposed an interpretation of the term "facility" in the FISA statute that was broader than how the term was ordinarily, but

²⁸⁰ The Department's application provided an example to illustrate the risks associated with the existing requirement that FISA Court approval or Attorney General emergency authorization be obtained each time the government seeks to target a particular telephone number or e-mail address: [redacted]

[redacted] According to the application, valuable intelligence could be lost in the time it would take to receive FISA Court authorization or Attorney General emergency authorization to target the new address. ~~(TS//SI//NF)~~

not always, applied.²⁸¹ Section 1805(a)(3)(B) of FISA provides that the Court may order electronic surveillance only upon finding that there is probable cause to believe that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by" a group involved in international terrorism. The term "facilities" generally was interpreted to refer to individual telephone numbers or e-mail addresses at which surveillance is "directed."~~(TS//SI//NF)~~

The government proposed in its content application that the term "facilities" be interpreted broadly to include [REDACTED]

[REDACTED]²⁸² Under this approach, instead of examining the target's use of particular telephone numbers or e-mail addresses, the Court would determine only whether there was probable cause to believe that the target was using [REDACTED] to communicate telephonically or by e-mail.²⁸³ ~~(TS//STLW//SI//OC/NF)~~

Second, the government's application requested that senior NSA officials be authorized to make individualized findings of probable cause about whether a particular telephone number or e-mail address was being used by a member or agent of one of the application's targets. Ordinarily, a FISA Court judge makes this probable cause determination. ~~(TS//SI//NF)~~

To implement this transfer of authority, the government proposed that NSA officials make the probable cause determinations as part of requirements called "minimization procedures," which are detailed rules

²⁸¹ The government's Memorandum of Law filed in support of the content application described several instances where the FISA Court authorized surveillance of facilities that was not limited to particular telephone numbers and e-mail addresses. According to the application [REDACTED]

The government's proposed interpretation of the term in the content application was far broader than previously authorized by the Court. ~~(TS//SI//NF)~~

²⁸² [REDACTED]

[REDACTED]

b1,
b3,
b7E

²⁸³ As noted, the targets of the content application were [REDACTED]. The government's content application included a declaration from the NSA Director that addressed [REDACTED] use of the international telephone system and [REDACTED] communications. ~~(TS//SI//NF)~~

b1,
b3,
b7E

that govern how the government must handle communications that it intercepts pertaining to U.S. persons. The FISA statute provides that each FISA application must include, and the FISA Court must approve, minimization procedures that the agency will follow with respect to communications intercepted pursuant to a FISA Court order. ~~(TS//SI//NF)~~

Minimization procedures, in the FISA context, ordinarily govern the handling of intercepted communications involving U.S. persons after the acquisition has been approved by the FISA Court. In other words, a FISA Court authorizes the agency to intercept the communications of particular selectors, and the agency follows the minimization procedures with respect to how it retains, uses, and disseminates any U.S. person information it collects under the Court's order. ~~(TS//SI//NF)~~

However, the government proposed as part of the content application that the minimization procedures also encompass how the NSA acquires the communications.²⁸⁴ Specifically, the application proposed that the NSA could intercept the communications of specific selectors if agency officials determined there was probable cause to believe that (1) the selector is being used by a member or agent of a [REDACTED] and (2) the communication is to or from a foreign country. The application referred to this as the "minimization probable cause standard."²⁸⁵ ~~(TS//SI//NF)~~

b1, b3,
b7E

Thus, the content application had a two-prong "minimization probable cause standard": (1) probable cause to believe a selector is being used by a member or agent of a targeted group, and (2) probable cause to believe the communication intercepted is to or from a foreign country. [REDACTED]

²⁸⁴ Bradbury told the OIG that this argument was based on the text of the FISA statute, which states that minimization procedures apply to the "acquisition" of communications in addition to their retention and dissemination. See 50 U.S.C. § 1801(h)(1). Indeed, the government's Memorandum of Law filed in support of the content application described several cases in which the FISA Court authorized the government to conduct electronic surveillance that included minimization at the time of acquisition. According to the application, the cases involved surveillance broadly targeted [REDACTED] than those the government specifically sought to acquire: [REDACTED]

b1, b3,
b7E

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

²⁸⁵ The proposed "minimization probable cause standard" was in addition to the standard minimization procedures that accompany every FISA application submitted by the government and that have been long-approved by the FISA Court. ~~(TS//SI//NF)~~

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

For the first prong – probable cause to believe a selector is being used by a member or agent of a targeted group – NSA analysts would assess sources of “reliable intelligence,” defined in the application as information from a variety of domestic and foreign intelligence and law enforcement activities. Under the terms of the application, positive findings of probable cause would be recorded in a database and the assessment process would be subject to periodic internal review by NSA officials, including the NSA General Counsel and Inspector General. (TS//SI//NF)

For the second prong – probable cause to believe the communication intercepted is to or from a foreign country [REDACTED]

[REDACTED] For example, the application stated that there would be probable cause to believe [REDACTED]

b1,
b3,
b7E

286 With respect to e-mails, the application stated that [REDACTED]

[REDACTED] 287 (TS//STLW//SI//OC/NF)

286 The application acknowledged that communications intercepted at the “facilities” could include some calls where [REDACTED] in the United States, or where [REDACTED] in the United States (even where there is probable cause to believe that [REDACTED] the United States).

b1,
b3,
b7E

[REDACTED]

If the NSA had probable cause to believe one of the communicants was a member of [REDACTED] the call could be intercepted. The application stated that such communications would be handled in accordance with NSA’s standard minimization procedures that apply to all of the agency’s electronic surveillance activities. (TS//SI//NF)

287 As it did with telephone communications, the application acknowledged that the manner in which e-mail communications are routed would cause the NSA to collect some e-mail communications that in fact are between communicants wholly within the United States. (Cont’d.)

Thus, viewing the government's approach to both "facilities" and "minimization procedures" together, the December 13, 2006, content application asked the FISA Court to find probable cause to believe that

engaged in international terrorism, and that these groups use the international telephone system and the communications system

b1, b3,
b7E

Then, within these broad parameters authorized by the Court, NSA officials would make probable cause findings about whether individual telephone numbers or e-mail addresses are used by members or agents of

and whether the communications of those numbers and addresses are to or from a foreign country. If they were, the NSA could direct the telecommunications carriers to intercept the communications of those telephone numbers and e-mail addresses and provide them to the NSA.

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

Under the terms of the application, communications acquired by the NSA could be retained for 5 years, unless the Court approved retention for a longer period. The application also stated that the NSA expected to initially target telephone numbers and e-mail addresses used by members or agents or

b1,
b3,
b7E

(TS//SI//NF)

An additional aspect of the content application is important to understand. The "early warning system" the government proposed applied both to "domestic selectors" and "foreign selectors." Domestic selectors are telephone numbers and e-mail addresses reasonably believed to be used by individuals in the United States; foreign selectors are telephone numbers and e-mail addresses reasonably believed to be used by individuals outside the United States. Under Stellar Wind, the NSA intercepted the communications of both categories of selectors, although the NSA tasked far more foreign selectors than domestic selectors. (TS//STLW//SI//OC/NF)

States, even though the NSA had probable cause to believe the communication was to or from a foreign country. The application stated that the NSA would handle any such communications in accordance with its standard minimization procedures. (TS//SI//NF)

The government proposed in its content application that the domestic selectors would be subject to more rigorous targeting approval and more frequent reporting to the FISA Court than foreign selectors, but the application sought to preserve NSA officials' authority to make the probable cause determinations as to each.²⁸⁸ As we describe below, the first FISA Court judge to consider the content application, Judge Malcolm Howard, was unwilling to extend this authority to domestic selectors. (TS//SI//NF)

C. Judge Howard Grants Application in Part (TS//SI//NF)

The Department's December 13, 2006, content application was assigned to Judge Howard, because he was the "duty" judge that week responsible for considering new applications.²⁸⁹ Judge Howard advised the Department orally that he would not authorize, on the terms proposed in the application, the electronic surveillance of selectors to be used by persons in the United States (domestic selectors). He did not issue a written opinion or order concerning this decision. The Department, in response to Judge Howard's oral advisement, filed a separate application requesting authority to conduct electronic surveillance on domestic selectors. This application, summarized below, was filed on January 9, 2007, and is considered the first "domestic selectors application"; the December 13 application is considered the first "foreign selectors application."
(TS//SI//NF)

Judge Howard also requested additional briefing from the Justice Department on the subject of whether [REDACTED] constituted "facilities" under FISA, and whether the surveillance authority sought in the government's content application would in fact be "directed" not at these "facilities" but rather at the particular telephone numbers and e-mail addresses the government would task for collection. (TS//SI//NF)

b1,
b3,
b7E

In response, the Department filed a supplemental memorandum of law on January 2, 2007, arguing that the government's construction of the

²⁸⁸ Under the terms of the original content application, domestic selectors tasked by the government would subsequently be reported to the Court for approval. The Court either had to approve each domestic selector within 48 hours of receiving the government's report or, if the Court did not agree there was probable cause to believe the selector was being used by a member or agent of a target of the application, provide the government 24 hours to submit additional information establishing probable cause. Foreign selectors tasked by the government did not require subsequent approval by the Court, although the Court could direct that the surveillance of any selector cease. (TS//SI//NF)

²⁸⁹ The Department offered to submit the application to the FISA Presiding Judge, Judge Kollar-Kotelly, but she said that it should be filed in the normal fashion, which meant it would be assigned to the FISA duty judge that week. (TS//SI//NF)

the Court found that the first prong of the standard has not been satisfied. In addition, the Order required the NSA Inspector General, General Counsel, and Signals Intelligence Directorate to periodically review the authorized collection activities. These NSA offices were required to submit a report to the Court 60 days after the collection was initiated under the Order that would address the adequacy of management controls and whether U.S. person information was being handled properly. ~~(TS//SI//NF)~~

According to several Department and NSA officials, the effort to implement Judge Howard's January 10, 2007, Order was a massive undertaking. [REDACTED]

b1, b3,
b7E

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

As a result of the Order, the Department and NSA submitted to the FISA Court for its review the factual basis for each selector supporting the government's determination that the "minimization probable cause standard" had been satisfied. The Department accomplished this pursuant to a schedule approved by Judge Howard under which the Department filed [REDACTED] foreign selectors every [REDACTED] days for the duration of the 90-day Order. ~~(TS//SI//NF)~~

b1,
b3,
b7E

The probable cause explanation for each foreign selector filed with the Court typically was described in several sentences. According to Bradbury, he impressed upon the NSA that Judge Howard would review each submission and inquire about how recently the NSA had acquired communications relating to a particular selector. According to Matthew Olsen, the Deputy Assistant Attorney General in the Department's National Security Division who was responsible for overseeing intelligence matters, Judge Howard did in some cases inquire about the government's factual basis for believing the minimization probable cause standard has been met.²⁹³ Bradbury also said he stressed that the Court would scrutinize the NSA's probable cause determinations more rigorously than the agency had been doing itself and that the Court was more likely to approve a selector where the surveillance was current than it would a selector that has "remained dormant for months."²⁹⁴ ~~(TS//SI//NF)~~

²⁹³ Olsen was involved in the drafting and presentation to the FISA Court of the content application and the government's implementation of the related FISA Court Orders. ~~(TS//SI//NF)~~

²⁹⁴ However, Bradbury noted that the FISA Court's "tendency to look for recent information" in assessing whether the probable cause standard has been met is "problematic" because [REDACTED]

(Cont'd.)

Olsen told us that [REDACTED] foreign selectors ultimately were filed with the FISA Court under the terms of Judge Howard's Order. Olsen said that the NSA strived to submit selectors that were deemed high priority, that had a well-documented nexus to [REDACTED] foreign powers, and that had recent communications activity. Attorneys from OIPR, who under the terms of the Order were required to review the NSA's justification for each foreign selector that it tasked, worked with the NSA on this large-scale review process. According to Olsen, OIPR attorneys "double-checked" the NSA's probable cause determination for each selector, but did not conduct independent probable cause inquiries. This review identified [REDACTED] selectors that in OIPR's judgment required additional documentation before they could be submitted to the Court.²⁹⁵ Olsen described the back-and-forth between OIPR and the NSA as "constant," and said the NSA was receptive to OIPR's involvement. Olsen stated that the NSA committed significant resources to the transition of foreign selectors. ~~(TS//SI//NF)~~

b1,
b3,
b7E

Both Bradbury and Olsen observed that the transition of content collection of foreign selectors to FISA required some adjustment by the NSA in its approach to establishing probable cause. For example, while an NSA analyst might base a probable cause determination to some extent on intuition, similar to a "cop on the beat," it was a different proposition when that probable cause determination had to be reviewed by several OIPR attorneys trying to anticipate how the FISA Court might view the judgment. Olsen stated that it was also "new" for the NSA to document the probable cause to the level OIPR believed the FISA Court would require. According to Bradbury, the effort sought an equilibrium between "the necessary speed and agility" and the "multiple layers of probable cause determination." Bradbury and Olsen both told the OIG that the NSA had concerns about whether the FISA approach to content collection would work and the extent to which a measure of effectiveness would be lost under FISA Court supervision. ~~(TS//SI//NF)~~

D. Domestic Selectors Application and Order ~~(TS//SI//NF)~~

In contrast to foreign selectors, Judge Howard advised the Justice Department that requests for surveillance of the international calls of domestic selectors – telephone numbers or e-mail addresses reasonably believed to be used by individuals in the United States – should be filed with

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

²⁹⁵ Olsen told the OIG that he believes the NSA de-tasked some of these foreign selectors. ~~(TS//SI//NF)~~

the Court in a separate application. Judge Howard also advised OIPR officials that any such application should take a more traditional approach to FISA, meaning the "facilities" targeted by the application should be particular telephone numbers and e-mail addresses and that the probable cause determination for tasking a selector would reside with the FISA Court, not with NSA officials pursuant to minimization procedures. (TS//SI//NF)

On January 9, 2007, the Department filed the first domestic selectors application. The application sought two things. First, the application requested authority to intercept the international communications of [REDACTED] specific domestic selectors.²⁹⁶ Second, the application sought, for purposes of future applications, approval to use a "streamlined version" of the emergency authorization procedures available under FISA. These emergency procedures authorize the use of electronic surveillance for a period of up to 72 hours without a Court order when the Attorney General reasonably determined that an emergency situation exists. See 50 U.S.C. § 1805(f). The procedures required the Attorney General to inform the FISA Court that the surveillance has been initiated and required the Department to file with the Court an emergency application to continue the surveillance not more than 72 hours after the surveillance was authorized. (TS//SI//NF)

b1, b3,
b7E

The goal of the Department's proposed streamlined emergency application procedures, referred to in the January 9, 2007, application as a "Verified Application," was to ensure that the emergency surveillance process be completed as swiftly as possible for qualifying domestic selectors. The proposal allowed the Verified Application to incorporate by reference the reasons or facts contained in the original domestic selectors application necessary to satisfy some of the statutory requirements under FISA, instead of reestablishing in each application for a new domestic selector that each of the requirements of FISA were met. The only new substantive information contained in a Verified Application would be the identity of the target, if known, the telephone number the target was using or was about to use, and the factual basis supporting probable cause to believe the target is [REDACTED] and is using or is about to use the identified telephone number. (TS//SI//NF)

Judge Howard granted the domestic selectors application on January 10, 2007, for a period of 90 days. His Order also approved the

²⁹⁶ Unlike the December 13, 2006, application, the January 9, 2007, application did not seek authority to target agents of [REDACTED] nor did the application seek authority to conduct content surveillance of e-mail communications. The declaration summarized for each of the domestic selectors, generally in two to three paragraphs, the facts that supported the government's belief that the telephone number was used or about to be used by a known or unknown agent of [REDACTED] located in the United States. (TS//SI//NF)

b1,
b3,
b7E

streamlined emergency authorization procedures proposed in the application for any additional domestic selectors whose communications the government sought to intercept during the 90-day period for which surveillance was authorized.²⁹⁷ ~~(TS//SI//NF)~~

NSD Deputy Assistant Attorney General Olsen told the OIG that in comparison with foreign selectors, the Department conducted a more rigorous review of the initial domestic selectors submitted to the FISA Court to ensure that probable cause was met. Olsen said a few domestic selector packages "on [their] face" lacked sufficient documentation and that these deficiencies were apparent to OIPR attorneys reviewing the information because the attorneys were looking at the information for the first time. He said that the NSA analysts responsible for the selectors, in contrast, were very familiar with the numbers and knowledgeable of details about the users that might not have been evident to persons reviewing documentation *de novo*. According to Olsen, for selector packages that were considered deficient, the NSA either provided the Justice Department attorneys with additional information or de-tasked the selector.²⁹⁸ ~~(TS//SI//NF)~~

E. Last Stellar Wind Presidential Authorization Expires
~~(TS//SI//NF)~~

On December 8, 2006, the President signed what would become the final Presidential Authorization for the Stellar Wind program. The December 8 Authorization was scheduled to expire on February 1, 2007. However, Judge Howard's January 10, 2007, Orders relating to foreign and domestic selectors completed the transition of Stellar Wind's

²⁹⁷ On January 22, 2007, the Department filed, and Judge Howard approved, the first Verified Application with the FISA Court using the streamlined procedures approved in the Order. ~~(TS//SI//NF)~~

²⁹⁸ Olsen and OIPR Deputy Counsel Margaret Skelly-Nolen told the OIG that during the application for and implementation of the domestic selectors Order, it became apparent that there were coordination problems between the FBI and the NSA. They noted that in many instances a domestic selector the NSA sought to task was already targeted by an FBI FISA order. According to Skelly-Nolen, in those cases problems can arise in providing accurate, current, and consistent information to the FISA Court about such selectors. She said the NSA's practice has been to consult with the FBI analysts assigned to the NSA and to request from them the most current information the FBI has about a particular telephone number or user of that number. The FBI analysts at the NSA have access to FBI databases to search for such information, although the most current information frequently can only be obtained from the operational personnel at FBI Headquarters. As a consequence, according to Skelly-Nolen, the FISA Court has on some limited occasions been provided inconsistent information concerning domestic telephone numbers or the users of those numbers. Olsen told the OIG that the domestic selectors Order has required a higher level of coordination between the FBI and NSA and that the National Security Division has worked to address this issue. ~~(TS//SI//NF)~~

communications and meta data collection activities from Presidential Authorization to FISA authority. Bradbury told the OIG that because it was believed that Judge Howard's Orders, particularly the foreign selectors Order, provided the NSA sufficient flexibility to conduct content collection, it was not necessary to renew the December 8, 2006, Presidential Authorization. ~~(TS//STLW//SI//OC/NF)~~

Therefore, on February 1, 2007, the Presidential Authorization for the Stellar Wind program officially expired.²⁹⁹ ~~(TS//SI//NF)~~

F. First Domestic and Foreign Selectors FISA Renewal Applications ~~(TS//SI//NF)~~

Judge Howard's January 10, 2007, Orders were set to expire after 90 days. During the week of March 20, 2007, the government filed renewal applications to extend the authorities both as to domestic and foreign selectors. These applications were filed with Judge Roger Vinson, the FISA Court duty judge that week. ~~(TS//SI//NF)~~

The domestic selectors application, filed March 22, 2007, was in all material respects identical to the government's original application. Judge Vinson granted the application on April 5, 2007.³⁰⁰ ~~(TS//SI//NF)~~

The foreign selectors application was filed on March 20, 2007. The content and construction of the March 20 application was substantially identical to the government's original application, and advanced the same broad construction of the term "facilities" and the use of minimization procedures to authorize NSA officials, instead of judges, to make probable cause determinations (subsequently reviewed by the FISA Court) about particular selectors. ~~(TS//SI//NF)~~

On March 29, 2007, Judge Vinson orally advised the Department that he could not grant the foreign selectors application. His decision validated some concerns within the Justice Department that Judge Howard's original

²⁹⁹ On January 17, 2007, Attorney General Gonzales sent a letter to Senators Leahy and Specter, the Chairman and Ranking Member of the Senate Judiciary Committee, informing them of Judge Howard's Orders. Gonzales's letter stated that as a result of the January 10, 2007, FISA Court Orders, any electronic surveillance that was occurring under the Terrorist Surveillance Program would now be conducted under FISA, and that "the President determined not to reauthorize the Terrorist Surveillance Program when the current authorization expires." ~~(TS//SI//NF)~~

³⁰⁰ As noted previously, the domestic selectors Order presented special coordination issues between the FBI and the NSA, and [REDACTED]. The Order was renewed for the final time in [REDACTED] and has since expired. ~~(TS//SI//NF)~~

Order might not be a sustainable long-term strategy for intercepting the communications of foreign selectors. Judge Vinson's decision also accelerated the Department's efforts to obtain legislation amending the FISA statute to authorize the type of surveillance conducted under Stellar Wind and that was approved by Judge Howard. (TS//SI//NF)

On April 3, 2007, Judge Vinson issued an Order and Memorandum Opinion explaining the reasoning for his conclusion that he could not grant the foreign selectors application. However, Judge Vinson did not deny the government's application. Instead, he encouraged the Department to file a motion with Judge Howard requesting a 60-day extension of the existing January 10, 2007, foreign selectors Order. In explaining why he was encouraging the Department to file the motion with Judge Howard, Judge Vinson wrote,

I have concluded that an extension for this purpose is appropriate, in view of the following circumstances: that the government has commendably devoted substantial resources to bring the NSA's surveillance program, which had been conducted under the President's assertion of non-FISA authorities, within the purview of FISA; that a judge of this Court previously authorized this surveillance in [the January 10, 2007, foreign selectors Order], on substantially the same terms as the government now proposes; that it would be no simple matter for the government to terminate surveillance of [REDACTED] phone numbers and e-mail addresses under FISA authority, and to decide whether and how it should continue some or all of the surveillance under non-FISA authority; and, importantly, that within the allotted time the government may be able to submit an application that would permit me to authorize at least part of the surveillance in a manner consistent with this order and opinion. (TS//SI//NF)

b1, b3, b7E

Judge Vinson wrote that the Department's foreign selectors renewal application concerns an "extremely important issue" regarding who may make probable cause findings that determine the individuals and the communications that can be subjected to electronic surveillance under FISA. In Judge Vinson's view, the question was whether probable cause determinations are required to be made by the FISA Court through procedures established by statute, or whether the NSA may make such determinations under an alternative mechanism cast as "minimization procedures." Judge Vinson concluded, based on past practice under FISA and the congressional intent underlying the statute, that probable cause determinations must be made by the FISA Court. (TS//SI//NF)

In explaining his reasoning, Judge Vinson first rejected the Department's broad construction of the term "facilities," concluding that the "electronic surveillance" under the government's application – the acquisition of the content of communications – was directed at particular telephone numbers and e-mail addresses, and not at broad swaths of communications

[REDACTED] as the government contended. Judge Vinson distinguished prior cases that the government cited for its broad interpretation of "facilities," observing, "[t]ellingly, none of the cited cases stand for the proposition on which this application rests – that electronic surveillance is not 'directed' at particular phone numbers and e-mail addresses, [REDACTED]

b1, b3,
b7E

[REDACTED] (TS//SI//NF) —

Judge Vinson wrote that his conclusion was also supported by the government's and the Court's past practice, as well as the legislative history of FISA, which, according to Judge Vinson, made clear that "Congress intended the pre-surveillance 'judicial warrant procedure,' and particularly the judge's probable cause findings, to provide an 'external check' on executive branch decisions to conduct surveillance." He wrote that the government's proposal that "the Court assess [REDACTED] and make a highly abstract and generalized probable cause finding [REDACTED]" removed from the Court's pre-surveillance purview the question of whether the communications to be acquired will relate to the targeted foreign powers.³⁰¹

(TS//SI//NF) —

Judge Vinson rejected the government's "minimization probable cause standard," stating that "[m]inimization does not provide a substitute for, or a mechanism for overriding, the other requirements of FISA." Judge Vinson concluded that government's proposed minimization procedures, by authorizing the NSA to make probable cause decisions, conflicted with specific provisions of FISA that govern electronic surveillance, such the requirement that only the Attorney General can grant emergency approvals to conduct surveillance (followed within 72 hours by an application to the

³⁰¹ Stated another way, "[the application] represented that NSA will make the required probable cause finding for each such facility before commencing surveillance." Judge Vinson wrote, "[t]he application seeks, in effect, to delegate to the NSA the Court's responsibility to make such findings 'based on the totality of circumstances.' Obviously, this would be inconsistent with the statutory requirement and the congressional intent that the Court make such findings prior to issuing the order (emphasis in original)."

(TS//SI//NF) —

FISA Court), and that renewals for surveillance coverage must be based on "new findings" of probable cause by a judge. Judge Vinson summarized his position:

The clear purpose of these statutory provisions is to ensure that, as a general rule, surveillances are supported by judicial determinations of probable cause before they commence; that decisions to initiate surveillance prior to judicial review in emergency circumstances are made at politically accountable levels; that judicial review of such emergency authorizations follows swiftly; and that decisions to continue surveillance receive the same degree of scrutiny as decisions to initiate. The law does not permit me, under the rubric of minimization, to approve or authorize alternative procedures to relieve the government of burdensome safeguards expressly imposed by the statute. (TS//SI//NF)

Judge Vinson wrote that he was mindful of the government's argument that the proposed minimization procedures were necessary to provide or enhance the "speed and flexibility" with which the NSA responds to threats, and that foreign intelligence information may be lost in the time it takes to obtain Attorney General emergency authorizations. However, in Judge Vinson's view, FISA's requirements reflected a balance struck by Congress between privacy interests and the need to obtain foreign intelligence information, and until Congress took legislative action on FISA to respond to the government's concerns, the Court must apply the statute's procedures.³⁰² He concluded that the government's application sought to strike a different balance for the surveillance of foreign telephone numbers and e-mail addresses. Vinson rejected this position, stating, "provided that the surveillance is within FISA at all, the statute applies the same requirements to surveillance of facilities used overseas as it does to surveillance of facilities used in the United States."³⁰³ (TS//SI//NF)

³⁰² Judge Vinson stated that he recognized that the government maintained the President may have constitutional or statutory authority to conduct the surveillance requested in the renewal application. Judge Vinson stated, "[n]othing in this order and opinion is intended to address the existence or scope of such authority, or this Court's jurisdiction over such matters." (TS//SI//NF)

³⁰³ Judge Vinson wrote in a footnote that the status of the proposed surveillance as being within the scope of FISA was "assumed, but not decided, for purposes of this order and opinion." He continued, "I believe that there are jurisdictional issues regarding the application of FISA to communications that are between or among parties who are all located outside the United States." Judge Vinson suggested that "Congress should also consider clarifying or modifying the scope of FISA and of this Court's jurisdiction with regard to such facilities" Bradbury told the OIG that Judge Vinson's suggestion was an important spur to Congress's willingness to consider FISA modernization legislation in

(Cont'd.)

Attorney General Gonzales told us that his reaction to Judge Vinson's decision was one of "disappointment" and that the decision "confirmed our concern about going to the [FISA Court]." Gonzales also said he believed the decision was "troubling for purposes of the national security of our country."

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

Bradbury told us the government considered several options after Judge Vinson's ruling, including appealing the decision to the FISA Court of Review. However, he said the decision was made to attempt to work with Judge Vinson to craft a revised application and also separately to renew the Administration's efforts to obtain legislation to modernize FISA.

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

G. Revised Renewal Application for Foreign Selectors and Order ~~(TS//SI//NF)~~

As suggested by Judge Vinson, in April 2007 the Justice Department obtained from Judge Howard an extension of the existing foreign selectors Order until May 31, 2007, to prepare a revised foreign selectors application. In the interim, the Department filed two reports with Judge Vinson describing a new approach to foreign selectors that addressed the concerns expressed in his Opinion, and that sought input from the Court about how best to facilitate the submission of an application that would seek authority to direct surveillance at [REDACTED] selectors. ~~(TS//SI//NF)~~

On May 24, 2007, the Department filed a revised renewal application seeking to renew, with modifications, the authorities granted in Judge Howard's January 10, 2007, Order. However, the application did not include the broad construction of "facilities" and instead sought authority to conduct electronic surveillance of conventional facilities - telephone numbers and "e-mail [REDACTED]." ³⁰⁴ The application also did not include the "probable cause minimization standard" approved

the summer of 2007. In Section IV below, we summarize this legislation, the Protect America Act, and its successor, the FISA Amendments Act of 2008. ~~(TS//SI//NF)~~

³⁰⁴ According to the May 24, 2007, application, such uses include Internet communications that are sent to and from a targeted e-mail "address," [REDACTED]

[REDACTED] The May 24 application was the [REDACTED] to use the term "e-mail [REDACTED]" to describe the facility at which e-mail surveillance would be directed;

However, according to the application, the government "routinely requests, and the Court authorizes, electronic surveillance using [the e-mail [REDACTED]] descriptor to identify this type of facility." ~~(TS//STLW//SI//OC/NF)~~

by Judge Howard that had the effect of shifting from the FISA Court to the NSA the probable cause determinations about particular selectors.

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

However, the targets of the government's revised application remained selectors (telephone number and e-mail facilities) reasonably believed to be used outside the United States and for which there is probable cause to believe were being used, or are about to be used, by [REDACTED]

b1, b3,
b7E

[REDACTED] ³⁰⁵ The application also sought [REDACTED] and in the same manner as was approved in Judge Howard's Order.³⁰⁶ ~~(TS//SI//NF)~~

Specifically, the application requested authority to direct surveillance at [REDACTED] categories of foreign selectors:

- o Foreign telephone number and e-mail selectors presently known to the government. This category accounted for a portion of the [REDACTED] foreign selectors already under surveillance pursuant to Judge Howard's Order.³⁰⁷

[REDACTED]

³⁰⁵ The May 24, 2007, application explicitly stated that the government was not seeking surveillance authority for any new facilities reasonably believed by the NSA to be used by U.S. persons. The application stated that surveillance of those facilities would be initiated only through FISA's emergency authorization provisions and the streamlined FISA applications approved for domestic selectors. ~~(TS//SI//NF)~~

³⁰⁶ [REDACTED]

b1,
b3,
b7E

³⁰⁷ The government submitted an appendix with the revised renewal application that identified [REDACTED] facilities and contained the factual basis for the NSA's belief that each of the facilities was being used by a person outside the United States and for which there was probable cause to believe were being used or about to be used by a member or agent of one of the targeted foreign powers. The government had provided Judge Vinson these facilities on a rolling basis during May 2007 for his consideration. The NSA discontinued the surveillance of facilities that were targeted under Judge Howard's Order, but that were not included among the facilities submitted to Judge Vinson for approval. The NSA told the OIG that the decision to discontinue surveillance on these [REDACTED] facilities largely was a resource decision and that [REDACTED] facilities figure was the amount the NSA could timely process for filing with the Court. ~~(TS//SI//NF)~~

b1, b3,
b7E

- Foreign e-mail selectors (not telephone number selectors) presently unknown to the government but that “refer to” or are “about” known foreign e-mail selectors. This category of surveillance, which the NSA had been conducting under Judge Howard’s Order, includes situations where an already targeted e-mail facility is mentioned in the body of a message between two third-party, non-targeted facilities.³⁰⁸ (TS//SI//NF)

According to the application, the [REDACTED] of surveillance would enable the NSA to initiate surveillance of newly discovered facilities “with the speed and agility necessary to obtain vital intelligence and to detect and prevent terrorist attacks.” The application stated,

[REDACTED]

The collection authorities requested in the renewal application that pertained to currently unknown facilities would, according to the application, address this limitation.³⁰⁹ (TS//SI//NF)

Judge Vinson granted the government’s revised renewal application on May 31, 2007. His Order authorized, for a period of 90 days, each of the [REDACTED] categories of electronic surveillance described above, although the

³⁰⁸ The category presented an issue under FISA in that communications are being acquired because they contain the targeted e-mail selector, and not because there was probable cause to believe the e-mail accounts sending or receiving the communications are used or about to be used by an international terrorist group. In such cases, the surveillance is not “directed at” the targeted e-mail selector. The government argued that such acquisition was still consistent with FISA because, “at the time of acquisition, the NSA has probable cause to believe that the facilities at which the NSA is directing surveillance are being used by the foreign power target.” (TS//SI//NF)

³⁰⁹ The government argued that the FISA Court’s authority to authorize subsequent collection against new selectors unknown to the government at the time an application was approved is rooted in section 1805(c)(3) of FISA. That provision imposes specific reporting requirements on the government where the FISA Court approves an electronic surveillance in circumstances where the nature and location of each of the facilities at which surveillance will be directed is unknown at the time of the application. (TS//SI//NF)

Order defined the precise circumstances under which the NSA could acquire communications falling within the [REDACTED] category of surveillance.³¹⁰ The Order also included reporting schedules with respect to the [REDACTED] categories of surveillance, for which the government was required to submit newly discovered selectors to the Court. ~~(TS//SI//NF)~~

Judge Vinson initially approved [REDACTED] foreign selectors under the terms of his May 31, 2007, Order (these selectors were submitted with the government's May 24, 2007, application). Shortly after the Order was issued, the FISA Court decided that the weekly reports filed by the government notifying the Court of newly discovered selectors, as well as the government's motions seeking approval to conduct surveillance on additional selectors, could be filed for review with any member of the Court. As the government received feedback from judges on the first reports and motions that were filed, it observed that judges were applying a more rigorous standard of review to the factual basis supporting the surveillance for each selector than Judge Vinson applied to the [REDACTED] selectors he approved. The government consequently adjusted the amount of factual information it provided the FISA Court in subsequent reports and motions and ultimately added [REDACTED] foreign selectors to Judge Vinson's Order. ~~(TS//SI//NF)~~

b1, b3,
b7E

According to Bradbury, the more rigorous scrutiny applied by FISA Court judges after Judge Vinson's initial approval [REDACTED] foreign selectors caused the NSA place only a fraction of the foreign selectors under coverage than it wanted to. This concern, combined with the comparatively laborious process for targeting foreign selectors under Judge Vinson's Order, accelerated the government's efforts to obtain legislation that would amend FISA to address the government's surveillance capabilities within the United States directed at persons located outside the United States. The Protect America Act, signed into law on August 5, 2007, accomplished this objective

b1, b3,
b7E

310

[REDACTED] However, his Order authorized the surveillance of any previously non-targeted e-mail facilities that transmitted e-mail messages containing a targeted e-mail account only when the NSA determined, based on the acquired communication and other intelligence or publicly available information, that there was probable cause to believe the e-mail facility was being used, or was about to be used, by one of the targeted foreign powers. Judge Vinson agreed with the government's position that there was probable cause to believe that Internet communications relating to a previously targeted e-mail facility were themselves being sent or received by one of the targeted foreign powers and could be acquired. Judge Vinson called this holding "novel," but concluded that the decision was "consistent with the overall statutory requirements; it requires the government to promptly report and provide appropriate justification to the Court; and it supplies the Government with a necessary degree of agility and flexibility in tracking the targeted foreign powers." ~~(TS//SI//NF)~~

b1, b3,
b7E

and effectively superseded Judge Vinson's foreign selectors Order. The government therefore did not seek to renew the Order when it expired on August 24, 2007. ~~(TS//SI//NF)~~

In the next section, we summarize the effect of the Protect America Act and successor legislation, the FISA Amendments Act of 2008. (U)

IV. **The Protect America Act and the FISA Amendments Act of 2008 (U)**

In August 2007, the Protect America Act was enacted, amending FISA to address the government's ability to conduct electronic surveillance in the United States of persons reasonably believed to be located outside the United States. This legislation expired on February 1, 2008, but was extended by Congress to February 16, 2008. In July 2008, the FISA Amendments Act of 2008 was enacted, which, among other things, created a comprehensive process under FISA for content collection directed at foreign targets. These two laws modernized the FISA statute as it applied to the acquisition in the United States of communications of persons reasonably believed to be outside the United States. (U)

As discussed in Chapter Three, FISA was enacted in 1978 when most international calls were carried by satellite. The interception of such calls constituted "electronic surveillance" for purposes of FISA only if the acquisition intentionally targeted a U.S. person in the United States, or if all participants to the communication were located in the United States. Thus, government surveillance of satellite communications that targeted foreign persons outside the United States generally was not considered electronic surveillance, and the government was not required to obtain a FISA Court order authorizing the surveillance even if one of the parties to the communication was in the United States. However, in the mid-1980s, fiber optic technology began to replace satellites as the primary means for transmitting international (and domestic) telephone communications. This change brought within FISA's definition of "electronic surveillance" the acquisition of telephone calls to or from a person in the United States if the acquisition occurred in the United States, thereby triggering the requirement that the government obtain FISA Court orders to conduct surveillance that it previously conducted outside of FISA. ~~(TS//SI//NF)~~

Under the Stellar Wind program, the NSA collected international communications [REDACTED] by targeting facilities (telephone numbers and e-mail addresses) located outside the United States (foreign

b1, b3,
b7E

selectors).³¹¹ As noted in Chapters Three and Four, the Administration contended that FISA, as supplemented by a subsequent legislative enactment (the AUMF), did not preclude the surveillance activities under Stellar Wind, or in the alternative represented an unconstitutional infringement on the President's Article II authority as Commander in Chief to the extent it conflicted with these collection activities.

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

The Justice Department's effort to transfer content collection from presidential authority under Stellar Wind to FISA raised the issue of FISA's application to the acquisition in the United States of communications to or from targeted foreign selectors. The Protect America Act and the FISA Amendments Act, in slightly different ways, addressed this issue by treating the communications of persons reasonably believed to be located outside the United States differently from communications of persons located in the United States.³¹² ~~(TS//STLW//SI//OC/NF)~~

A. The Protect America Act (U)

The Protect America Act of 2007, Pub. L. No. 110-55, was a temporary measure signed into law on August 5, 2007.³¹³ The Protect America Act's chief objective was to exclude from the requirements of FISA the interception in the United States of communications of persons located outside the United States, the category of communications referred to above as "foreign selectors." (U)

The Protect America Act amended FISA so that the interception of foreign selector communications fell outside the statute's definition of "electronic surveillance." Under the original definition of "electronic surveillance," FISA generally applied to any communication to or from a known United States person inside the United States if the communication is acquired by targeting the known United States person.³¹⁴ FISA also

³¹¹ The NSA also targeted under Stellar Wind a much smaller number of facilities located inside the United States (domestic selectors). ~~(TS//STLW//SI//OC/NF)~~

³¹² The two laws did not substantially affect the provisions of FISA relating to pen register and trap and trace surveillance or to the production of "tangible things." The government continues to collect bulk e-mail and telephone meta data under the PR/TT and Section 215 Orders described in Sections I and II of this chapter. ~~(TS//SI//NF)~~

³¹³ The Protect America Act was set to expire 180 days after its enactment, or on February 1, 2008. However, Congress passed and on January 31, 2008, the President signed a bill to extend the Protect America Act for 15 days while further discussions on new legislation occurred. However, no agreement was reached on new legislation and the Act expired on February 16, 2008. (U)

³¹⁴ The original FISA definition of "electronic surveillance" included:

(Cont'd.)

applied to the acquisition of other communications (such as communications acquired by targeting persons outside the United States) if the communication was a "wire communication" and the acquisition occurred inside the United States. (U)

The Protect America Act amended FISA by stating: "Nothing in the definition of electronic surveillance . . . shall be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States." The effect of this amendment was to exclude from the requirements of FISA any communication acquired by targeting a foreign selector, regardless of where the communication was intercepted or whether the communication traveled by wire. As a result, the Act eliminated the need for Judge Vinson's May 2007 foreign selectors Order, because the collection of communications targeted under that Order no longer constituted "electronic surveillance" under FISA and therefore no longer required FISA Court orders.³¹⁵ ~~(TS//SI//NF)~~

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(20)(i) of Title 18;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

50 U.S.C. § 1801(f). (U)

315

(Cont'd.)

In the place of individualized FISA Court orders, the Protect America Act also inserted several provisions into the FISA statute to govern the acquisition of communications from persons "reasonably believed to be outside the United States." These provisions authorized the Attorney General and the Director of National Intelligence to acquire foreign intelligence information concerning such persons for up to one year, provided these officials certified that there are reasonable procedures in place for the government to determine that a target is reasonably believed to be outside the United States and that the acquisition of the foreign intelligence therefore is not "electronic surveillance" under the amended definition of the term.³¹⁶ The targeting procedures accompanying the certification had to be submitted to the FISA Court for approval, based on the clearly erroneous standard, within 120 days of the Protect America Act's enactment. However, the certification was not required to identify specific facilities or places at which the acquisition of foreign intelligence information would be directed.³¹⁷ (U)

In addition, the Protect America Act authorized the Attorney General and the Director of National Intelligence to direct a person (telecommunications carriers) to provide the government with "all information, facilities, and assistance necessary to accomplish the acquisition in such a manner as will protect the secrecy of the acquisition. . . ." Protect America Act, Sec. 2(e). The Protect America Act also authorized the Attorney General and the Director of National

[REDACTED] The Protect America Act addressed this issue by excluding all surveillance directed at persons reasonably believed to be outside the United States.

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

³¹⁶ The Attorney General and the Director of National Intelligence also had to certify that the acquisition involves the assistance of a communications service provider; that a "significant purpose" of the acquisition to obtain foreign intelligence information is for foreign intelligence purposes; and the minimization procedures to be used with the acquisition activity comport with 50 U.S.C. § 1801(h). Protect America Act, Sec. 2, codified in FISA at 50 U.S.C. § 1805B(a)(1)-(5). (U)

³¹⁷ The Protect America Act left unchanged the procedures for acquiring foreign intelligence information by targeting foreign powers or agents of foreign power inside the United States, as well as the procedures under Executive Order 12333 Sec. 2.5 to obtain Attorney General approval before acquiring foreign intelligence information against a U.S. person outside the United States. Thus, FISA orders issued prior to the enactment of the Protect America Act, and FISA orders, including applications for renewals, sought after enactment of the Protect America Act but not pursuant to the Act's amendments (acquisition of foreign intelligence information from targets outside the United States) were still subject to FISA as it existed prior to the Protect America Act. The Protect America Act also provided, by means of an "opt-out" clause, that the government did not have to use the new procedures for new applications and could instead file applications under the provisions of FISA as it existed before the Protect America Act. See Protect America Act, Sec. 6(b). (U)

Intelligence to seek the assistance of the FISA Court to compel compliance with such directives, and implemented procedures for the telecommunications carriers to challenge the legality of any such directives.³¹⁸ (U)

The Protect America Act authorized the Attorney General and the Director of National Intelligence to issue orders without individualized FISA Court approval for up to one year targeting persons reasonably believed to be outside the United States. These orders remained in effect beyond the expiration of the Protect America Act on February 16, 2008. (U)

On August 10, 2007, the Attorney General and the Director of National Intelligence filed a certification with the FISA Court, as required under the Protect America Act, relating to surveillance of persons reasonably believed to be outside the United States likely to communicate information concerning [REDACTED]

[REDACTED] The certification included directives for assistance to specific telecommunications carriers. ~~(TS//SI//NF)~~

b1,
b3,
b7E

[REDACTED] foreign selectors under Judge Vinson's Order were "rolled over" to the new Protect America Act authority. A Deputy Assistant Attorney General in the National Security Division familiar with the transition of Stellar Wind to FISA Court authority told us that the government also began to "build new selectors" under the Protect America Act and worked toward restoring the universe of foreign selectors that were first authorized for tasking under Judge Howard's January 2007 Order when content collection under Stellar Wind initially had migrated to FISA Court authority. ~~(TS//SI//NF)~~

b1,
b3,
b7E

Although the Department viewed the Protect America Act as an adequate temporary fix to those provisions of FISA seen as outdated because of changes in telecommunications technology, Department officials continued to press Congress for more permanent modernization legislation. (U)

³¹⁸ The Protect America Act also stated that any person providing assistance to the government pursuant to a governmental directive would not be subject to any cause of action for providing such assistance. However, the Protect America Act did not grant retroactive legal immunity to any "person," a term defined in FISA to include "any group, entity, association, corporation, or foreign power." 50 U.S.C. § 1801(m). On August 22, 2008, the FISA Court of Review upheld as constitutional the Protect America Act provision authorizing the Director of National Intelligence and the Attorney General to direct a person to assist the government in implementing the Act. See In Re: Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, No. 08-01. (U)

B. The FISA Amendments Act of 2008 (U)

On July 11, 2008, the President signed the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FISA Amendments Act). This legislation, composed of four titles, replaced the Protect America Act with similar but more comprehensive surveillance authority. The provisions of the FISA Amendments Act expire, with limited exceptions, on December 31, 2012. (U)

A chief objective of the FISA Amendments Act was to change the rules for intercepting the electronic communications of persons reasonably believed to be outside the United States when the acquisition occurs in the United States. As discussed above, the Protect America Act accomplished this by amending FISA's definition of "electronic surveillance" to exclude this activity from FISA requirements. The FISA Amendments Act took a different approach. Instead of excluding the activity from the statute's definition of "electronic surveillance," the FISA Amendments Act created a new title in FISA to govern how the government may conduct this electronic surveillance. Under this approach, the FISA Amendments Act, unlike the Protect America Act, distinguishes between the targeting of non-U.S. and U.S. persons reasonably believed to be outside the United States.³¹⁹ (U)

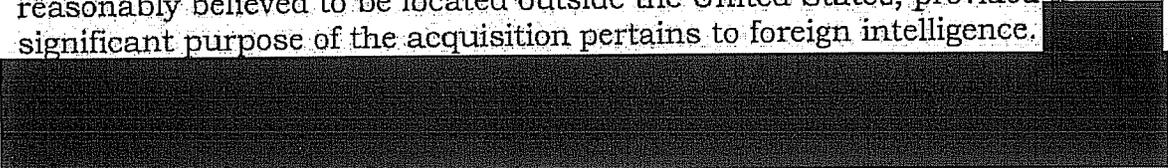
For non-U.S. persons, the new title created by the FISA Amendments Act provides for surveillance authority similar to the Protect America Act. Instead of requiring the government to obtain individualized orders from the FISA Court to intercept communications of non-U.S. persons reasonably believed to be outside the United States, the FISA Amendments Act authorized the government to conduct any such interceptions for a period of up to one year provided that it adopts, and the FISA Court approves, general targeting procedures designed to ensure that the new authority is not used

³¹⁹ The Senate Select Committee on Intelligence (SSCI) prepared a section-by-section analysis of the FISA Amendments Act of 2008 explaining the significance of the FISA Amendment Act's approach. According to the SSCI report, the goal of the Protect America Act in redefining the term "electronic surveillance" was to exclude the surveillance of persons outside the United States from the individualized order requirements of FISA. However, a consequence of the term's redefinition was to broadly exempt foreign surveillance activities both of non-U.S. and U.S. persons outside the United States. The FISA Amendments Act of 2008, instead of adopting the Protect America Act's modified definition of "electronic surveillance," explicitly stated that the targeting of non-U.S. persons outside the United States shall be conducted under the new FISA procedures, which does not require an application for a FISA order. In this way, the FISA Amendments Act accomplished the same goal as the Protect America Act without exempting the targeting of U.S. persons outside the United States from FISA's individualized order requirements. (U)

to direct surveillance at persons within the United States or at U.S. persons outside the United States.³²⁰ (U)

In contrast, to conduct U.S.-based surveillance of U.S. persons reasonably believed to be located outside the United States, the FISA Amendments Act requires the government to obtain individualized FISA Court orders for 90-day periods based on a showing of probable cause to believe that the U.S. person is outside the United States and is a foreign power or an agent, officer, or employee of a foreign power. Such surveillance previously was governed by Executive Order 12333, and required only a certification from the Attorney General, not the FISA Court. (U)

Compared to Stellar Wind, the FISA Amendments Act provides the government broader authority to acquire in the United States, with Court supervision, the communications of non-U.S. persons reasonably believed to be located outside the United States. Under Stellar Wind, the NSA was authorized to collect communications where there was probable cause to believe the communications originated or terminated outside the United States and a party to the communications was al Qaeda or a group affiliated with al Qaeda. Under the FISA Amendments Act, the NSA is authorized to collect in the United States any communications of non-U.S. persons reasonably believed to be located outside the United States, provided a significant purpose of the acquisition pertains to foreign intelligence.



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

³²⁰ Like the Protect America Act, in addition to these targeting procedures the certification the government is required to file with the FISA Court must also contain minimization procedures and state that a significant purpose of the acquisition that will be conducted is to obtain foreign intelligence information. However, unlike the Protect America Act the FISA Amendments Act does not limit the FISA Court's review of the targeting procedures to a "clearly erroneous" standard. On August 5, 2008, the government submitted to the FISA Court a certification pursuant to the FISA Amendments Act. On September 5, 2008, the Court approved the certification and the use of the targeting and minimization procedures the government submitted. ~~(S//NF)~~

³²¹ On the other hand, the FISA Amendments Act does not similarly broaden the government's authority to conduct surveillance of U.S. persons reasonably believed to be located outside the United States. The Presidential Authorizations did not distinguish between U.S. and non-U.S. persons, and the NSA was authorized under Stellar Wind to intercept the communications of U.S. persons (domestic selectors) provided the communications originated or terminated outside the United States.

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

In Chapter Three, we noted that under certain circumstances technological limitations associated with the e-mail content aspect of the Stellar Wind program caused [REDACTED]

[REDACTED]

(TS//SI//NF)

The NSA undertook measures to identify and correct incidents [REDACTED] under Stellar Wind, and the government described the issue to the FISA Court in the December 2006 application that sought to bring Stellar Wind's content collection under FISA authority [REDACTED]

[REDACTED]

(TS//SI//NF)

[REDACTED]