

17-3399

IN THE
United States Court of Appeals
FOR THE
Second Circuit

AMERICAN CIVIL LIBERTIES UNION and AMERICAN CIVIL LIBERTIES UNION FOUNDATION,
Plaintiffs–Appellants,

– v. –

NATIONAL SECURITY AGENCY, CENTRAL INTELLIGENCE AGENCY, UNITED STATES
DEPARTMENT OF DEFENSE, UNITED STATES DEPARTMENT OF JUSTICE, and
UNITED STATES DEPARTMENT OF STATE,
Defendants–Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

JOINT APPENDIX: VOLUME 2 OF 2 (JA243–JA489)

Hannah Bloch-Wehba
David Schulz
Sebastian Brady (law student intern)
Diana Lee (law student intern)
Paulina Perlin (law student intern)
Media Freedom and Information Access
Clinic, Abrams Institute,
Yale Law School
P.O. Box 208215
New Haven, CT 06520
Phone: (212) 850-6103
hannah.bloch-wehba@yale.edu

Ashley Gorski
Patrick Toomey
American Civil Liberties Union
Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
agorski@aclu.org

Counsel for Plaintiffs–Appellants

*American Civil Liberties Union, et al. v. National Security Agency, et al.,
No. 17-3399 (2d Cir.)*

**JOINT APPENDIX
TABLE OF CONTENTS**

Volume 1

U.S. District Court for the Southern District of New York, Docket
Sheet, Case No. 1:13-cv-09198-KMWJA001

Stipulation and Order Regarding Document Searches (May 9, 2014),
ECF No. 30JA017

Plaintiffs’ Second Amended Complaint (Oct. 31, 2014),
ECF No. 44JA024

Declaration of David J. Sherman, Associate Director for Policy and
Records at the National Security Agency (Feb. 26, 2016), ECF
Nos. 64, 64-1, & 64-14JA136

Declaration of John Bradford Wiegmann, Deputy Assistant Attorney
General in the National Security Division of the Department of
Justice (Feb. 26, 2016), ECF Nos. 65 & 65-1JA183

Volume 2

Declaration of Paul P. Colborn, Special Counsel in the Office of
Legal Counsel of the Department of Justice (Feb. 26, 2016), ECF
Nos. 67, 67-1, & 67-5–67-11JA243

Declaration of Jonathan Manes, attorney, Yale Media Freedom and
Information Access Clinic (Apr. 20, 2016), ECF Nos. 71 & 71-6JA417

Notice of Filing of Classified NSA Declaration (June 8, 2016),
ECF No. 74JA447

Second Declaration of David J. Sherman, Associate Director for Policy and Records at the National Security Agency (June 8, 2016), ECF No. 79JA449

Second Declaration of John Bradford Wiegmann, Deputy Assistant Attorney General in the National Security Division of the Department of Justice (June 8, 2016), ECF No. 80JA458

Third Declaration of David J. Sherman, Associate Director for Policy and Records at the National Security Agency (June 14, 2017), ECF No. 103JA465

Declaration of Kevin G. Tiernan, Supervisory Records Manager, National Security Division of the Department of Justice (June 14, 2017), ECF No. 104JA475

Notice of Appeal (Oct. 20, 2017), ECF No. 114JA488

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

AMERICAN CIVIL LIBERTIES UNION, and
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY,
CENTRAL INTELLIGENCE AGENCY,
DEPARTMENT OF DEFENSE,
DEPARTMENT OF JUSTICE, and
DEPARTMENT OF STATE,

Defendants.

13 Civ. 9198 (AT)

DECLARATION OF PAUL P. COLBORN

I, Paul P. Colborn, declare as follows:

1. I am a Special Counsel in the Office of Legal Counsel (“OLC”) of the United States Department of Justice (the “Department”) and a career member of the Senior Executive Service. I joined OLC in 1986, and since 1987 I have had the responsibility, among other things, of supervising OLC’s responses to requests it receives under the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552. I submit this declaration in support of the Department’s Motion for Summary Judgment in this case. The statements that follow are based on my personal knowledge, as well as on information provided to me by OLC attorneys and staff working under my direction, and by others with knowledge of the documents at issue in this case. This declaration incorporates by reference the index of documents withheld in full or in part by OLC attached hereto as Exhibit A.

JA243

OLC'S RESPONSIBILITIES

2. The principal function of OLC is to assist the Attorney General in her role as legal adviser to the President of the United States and to departments and agencies of the Executive Branch. OLC provides advice and prepares opinions addressing a wide range of legal questions involving the operations of the Executive Branch. OLC does not purport to make policy decisions, and in fact lacks authority to make such decisions. OLC's legal advice and analysis may inform the decisionmaking of Executive Branch officials on matters of policy, but OLC's legal advice is not itself dispositive as to any policy adopted.

3. Although OLC publishes some opinions and makes discretionary releases of others, OLC legal advice is generally kept confidential. One important reason OLC legal advice often needs to stay confidential is that it is part of a larger deliberative process—a process that itself requires confidentiality to be effective. If government agencies and OLC had to conduct deliberations with knowledge that their deliberations were open to public view, such discussions would naturally be chilled or inhibited, and the efficiency of government policy making would suffer as a result.

4. These deliberative confidentiality concerns apply with particular force to OLC advice because of OLC's role in the decisionmaking process: OLC is often asked to provide advice and analysis with respect to very difficult and unsettled issues of law. Frequently, such issues arise in connection with highly complex and sensitive activities of the Executive Branch on matters that can be quite controversial. So that Executive Branch officials may continue to request, receive, and rely on candid legal advice from OLC on such sensitive matters, it is essential that OLC legal advice provided in the context of internal deliberations not be inhibited by concerns about public disclosure.

5. The foregoing considerations regarding the need for confidential Executive Branch deliberations are particularly compelling in the context of the provision of legal advice, given the nature of the attorney-client relationship. There is a special relationship of trust between a client and an attorney when the one seeks and the other provides independent legal advice. When the advice is provided in confidence, it is protected from compelled disclosure. As the Supreme Court has observed, “[t]he attorney-client privilege is the oldest of the privileges for confidential communications known to the common law. Its purpose is to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice.” *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981). It is critical to protect this relationship of trust in the governmental context, to ensure such full and frank communication between governmental attorneys and their clients, and thereby promote such broader public interests in the government’s observance of law and the administration of justice. The free and candid flow of information between agency decisionmakers and their outside legal advisers depends on the decisionmakers’ confidence that the advice they receive will remain confidential. Moreover, disclosure of legal advice may often reveal confidential communications from agency clients made for the purposes of securing advice.

6. When requested to provide counsel on the law, OLC attorneys stand in a special relationship of trust with their agency clients. Just as disclosure of client confidences in the course of seeking legal advice would seriously disrupt the relationship of trust so critical when attorneys formulate legal advice to their clients, disclosure of the advice itself would be equally disruptive to that trust. Thus, the need to protect the relationship of trust between OLC and the

client seeking its legal advice provides an additional reason OLC legal advice often needs to stay confidential.

7. The interests protected by the deliberative process and attorney-client privileges continue to apply fully to confidential OLC legal advice in circumstances where the Executive Branch or one of its departments or agencies elects, in the interest of transparency, to explain publicly the Executive Branch's understanding of the legal basis for current or contemplated Executive Branch conduct. There is a fundamental distinction between an explanation of the rationale and basis for a decision, which would not be privileged, and advice received prior to making a decision, which is privileged. Thus, there is no disclosure of privileged legal advice, and therefore no waiver of attorney-client privilege, when, as part of explaining the rationale for its actions or policies, the Executive Branch explains its understanding of their legal basis without reference to any confidential legal advice that Executive Branch decisionmakers may have received before deciding to take the action or adopt the policy. Likewise, confidential advice does not lose the protection of the deliberative process privilege simply because the Executive Branch explains the basis or rationale for its actions or policies without referring to that advice; rather, confidential deliberative advice loses this protection only through adoption, *i.e.*, if the advice is expressly adopted as part of the explanation of the rationale for the decision or waiver, *i.e.*, through specific voluntary disclosure of the deliberative material. If merely explaining publicly the legal basis for Executive Branch conduct were understood to remove the protection of the deliberative process and attorney-client privileges from the confidential legal advice provided as part of the Executive Branch's internal deliberations, it would substantially harm the ability of Executive Branch decisionmakers to request, receive, and rely upon full and frank legal advice from government lawyers as part of the decisionmaking process, and it would

also harm the public by discouraging the Executive Branch from explaining its understanding of the legal basis for its actions publicly in the future.

PLAINTIFFS' FOIA REQUEST

8. On May 29, 2013, OLC received a request dated May 13, 2013 from Alexander Abdo on behalf of the American Civil Liberties Union Foundation (together with the American Civil Liberties Union, hereinafter the "ACLU"), requesting records in three categories. *See* Ex. B, at 1 (FOIA Request (May 13, 2013)) (hereinafter, as modified, "the ACLU Request"). Those categories were as follows:

a. "Any records in which the Office of Legal Counsel ("OLC") construes or interprets the authority of the Department of Justice ('DOJ') or any executive agencies under Executive Order 12,333 or any regulations issued thereunder;" *Id.*

b. "Any records describing the minimization procedures used by the government with regard to both intelligence collection and intelligence interception conducted pursuant to EO 12,333 or any regulations issued thereunder; and" *Id.*

c. "Any records describing the standards that must be satisfied for the 'collection,' 'acquisition,' or 'interception' of communications, as those terms are defined in EO 12,333 or any regulations issued thereunder."

9. By letter dated June 25, 2013, I sent a letter to Mr. Abdo on behalf of OLC, acknowledging receipt of the ACLU Request and proposing a narrowing agreement following an earlier telephone conversation between Mr. Abdo and an OLC attorney. *See* Ex. C, at 1 (OLC Acknowledgment (June 25, 2013)).

10. On July 10, 2013, Mr. Abdo confirmed the narrowing agreement with certain modifications agreed to by email. *See* Ex. D, at 1 (Narrowing email (July 10, 2013)). As

modified and agreed to by OLC and the ACLU, the ACLU Request was narrowed to the following:

a. “All OLC final legal advice concerning Executive Order 12333 or its implementing regulations with respect to electronic surveillance by the United States Government of communications of United States persons, regardless of whether the United States person is the target of the electronic surveillance or is in the United States at the time of the electronic surveillance. For purposes of this request, ‘electronic surveillance’ and ‘United States person’ have the meaning given in Executive Order 12333.” *Id.*

b. “All OLC final legal advice concerning the meaning of the terms ‘collection’, ‘acquisition’, and ‘interception’ as used in Executive Order 12333 or its implementing regulations with respect to electronic surveillance by the United States Government of communications of United States persons. For purposes of this request, ‘electronic surveillance’ has the meaning given in Executive Order 12333.” *Id.*

11. On December 30, 2013, before OLC had completed its search, ACLU filed this lawsuit.

12. On September 22, 2014, following a search and pursuant to the parties’ stipulated scheduling order in this case, OLC informed Mr. Abdo that it had located ten responsive records. *See Ex. E, at 1 (OLC Response (Sept. 22, 2014))*. Of the ten records, OLC enclosed three with portions redacted and withheld seven in full. *Id.* Mr. Abdo was informed that the redactions and withholdings were made pursuant to FOIA Exemptions One, Three, and/or Five, 5 U.S.C. § 552(b)(1), (3), (5). *Id.* I understand that ACLU has designated a subset of various agencies’ responsive records as still at issue in this case, and has excluded some documents located by

other agencies, but continues to seek release of the ten documents that OLC located and withheld in full or in part.

13. In addition to the ten documents withheld by OLC and identified in the attached index, two documents were withheld on behalf of OLC by the Department's National Security Division ("NSD"), which I understand that ACLU continues to seek as well. These documents are identified as NSD 9 and NSD 36 in the index attached to the Declaration of John Bradford Wiegmann, filed contemporaneously herewith.

OLC'S SEARCH

14. I have been informed that the ACLU does not challenge the adequacy of OLC's search for responsive documents, and for that reason I do not describe the search here.

APPLICABLE PRIVILEGES

15. The withheld records consist primarily of memoranda authored by OLC containing OLC's confidential, predecisional legal advice to assist Executive Branch clients in making policy decisions. Accordingly, such records are covered by the deliberative process and/or attorney-client privileges, and therefore are exempt under FOIA Exemption Five, unless those privileges have been lost by waiver or adoption.

16. The deliberative process privilege protects documents that are (a) predecisional, in that they were generated prior to decisions or potential decisions; and (b) deliberative, in that they contain, reflect, or reveal advice, discussions, proposals, and the "give and take" exchanges that characterize the government's deliberative processes.

17. As discussed below, all but one of the fully or partially withheld records are protected by the deliberative process privilege in whole or in part. They are predecisional and deliberative, in that they consist of legal advice to Executive Branch decisionmakers. Requiring

disclosure of these documents would undermine the deliberative processes of the government and chill the candid and frank communications necessary for effective governmental decisionmaking. It is essential to OLC's mission and the deliberative processes of the Executive Branch that OLC's considered legal advice not be inhibited by concerns about the compelled public disclosure of predecisional matters, including factual information necessary to develop accurate and relevant legal advice. Protecting the withheld documents from compelled disclosure is central to ensuring that Executive Branch attorneys will be able to examine relevant facts and analysis, and provide candid, complete advice, and to ensuring that Executive Branch officials will seek legal advice from OLC and the Department of Justice on sensitive matters.

18. The attorney-client privilege protects documents that contain or reflect confidential legal advice provided by an attorney to a client, and confidential client requests for legal advice and other confidential communications and facts conveyed by the client to the attorney for the purpose of receiving legal advice.

19. As discussed below, all but one of the fully or partially withheld records are protected by the attorney-client privilege in whole or in part. These documents consist of legal advice that was communicated in confidence from OLC to Executive Branch clients, and disclose confidential client requests for legal advice. In addition, many of the documents also contain factual information that was communicated in confidence by Executive Branch clients to OLC for the purpose of obtaining confidential legal advice, and the existence of confidential legal advice documents reflects the privileged fact that a client requested confidential legal advice on a particular subject. Having been asked to provide legal advice, OLC attorneys stood in a relationship of trust with their Executive Branch clients. Just as disclosure of client confidences provided in the course of seeking legal advice would seriously disrupt the

relationship of trust so critical when attorneys formulate legal advice for their clients, so too would disclosure of the legal advice itself undermine that trust.

DOCUMENTS AT ISSUE

20. I am personally familiar with the withheld OLC documents that are at issue in this case. An index listing the ten OLC documents at issue is attached to this declaration, as are copies of the three redacted OLC documents that were released to the plaintiffs.

21. *OLC Advice Memoranda.* Ten of the twelve documents—Documents 2-8, and 10 in the attached index as well as NSD 9 and NSD 36—are classified OLC legal advice memoranda. These memoranda were written in response to confidential communications from one or more executive branch clients soliciting legal advice from OLC attorneys. As with all such OLC legal advice memoranda, these documents contain confidential client communications for the purpose of seeking legal advice and predecisional legal advice from OLC attorneys transmitted to executive branch clients as part of government deliberative processes. Documents 8 and 10 have been partially released in redacted form.

22. OLC’s withholding of three of these documents from the ACLU in response to a different FOIA request was upheld last year after *in camera* review by the United States District Court for the District of Columbia in the consolidated case *Elec. Privacy Info. Ctr. v. Dep’t of Justice*, Nos. 06- 096, 06-214 (RCL), 2014 WL 1279280 (D.D.C. Mar. 31, 2014) (“*EPIC*”); *See also* Second Redacted Bradbury Declaration, ECF No. 35-1, No. 06-214 (Filed Oct. 19, 2007) (describing these and other documents), attached hereto as Exhibit F (“Bradbury *EPIC* Declaration”). Document 4 was identified in that case as OLC 132, Document 8 was identified as OLC 131; and Document 10 was identified as OLC 54. *See* Bradbury *EPIC* Declaration ¶¶ 83(b), (g), (h). Each was among the ten opinions reviewed *in camera* and determined to be

properly withheld from disclosure to the ACLU pursuant to Exemptions One, Three, and Five. 2014 WL 1279280, at *1 (“The Court is now satisfied with the Department's decisions to withhold these ten records under Exemptions One and Three, since they are in fact properly classified, as well as Exemption Five as each record contains confidential, pre-decisional legal advice protected by the deliberative-process and attorney-client communications privileges.”).

23. While the *EPIC* litigation was pending, there was an interagency classification and privilege review of four of the documents at issue in that case, including the documents identified here as Documents 4, 8, and 10, which took approximately six months and culminated in the partial release to ACLU and the other *EPIC* plaintiffs of Documents 8 and 10, in redacted form, on March 18, 2011. Following the declassification of certain information contained in Document 10, there was another interagency review of that document, which again took approximately six months. In September 2014, pursuant to the interagency review, NSA informed the Department of Justice that OLC 10 contained classified and/or protected NSA equities and therefore that NSA was withholding that material from public disclosure pursuant to Exemptions One and Three of the FOIA. This second review culminated in a discretionary release of a revised version of Document 10 with fewer redactions in early September 2014—six months after the *EPIC* court's *in camera* review and determination that the documents were properly withheld in full or as redacted, including the portions of Document 10 that had been redacted and withheld pursuant to Exemptions One, Three, and Five. Shortly after the completion of this review process, the reprocessed version of Document 10 was provided to ACLU in OLC's September 22, 2014 response. *See supra* ¶ 12.

24. In September 2015, the Government made a partial release of a classified Office of Inspector General report regarding topics related to the subject matter of Document 10, as part

of a FOIA response in litigation in this District. *See N.Y. Times v. Dep't of Justice*, S.D.N.Y. No. 14-cv-3776 (AT). This September 2015 release included previously undisclosed material. Although it is possible that additional material disclosed in connection with the September 2015 release appears in portions of Document 10 redacted pursuant to Exemptions One, Three, and Five, that material was not appropriate for discretionary release at the time of OLC's administrative response to the requester on September 22, 2014. In light of Document 10's length and the fact that it has recently been the subject of a comprehensive interagency review for potential discretionary release, Document 10 has not been reviewed an additional time for any potential additional discretionary release following the September 2015 release. Similarly, pursuant to Executive Order 13526, ¶ § 3.5(d), Document 10 was not resubmitted for classification review at the time of OLC's administrative response to the requester on September 22, 2014 because such a review had just been concluded with material determined at that time by the NSA to be properly classified, and has not been resubmitted for declassification review because such a review was conducted within the past two years.

25. *Cover Memorandum.* One of the documents—Document 1 in the attached index—is a cover memorandum transmitting one of the legal advice memoranda (Document 2). This cover memorandum contains an unclassified partial summary of Document 2, including a description of the solicitation of advice and a summary of the memorandum's conclusions.

26. *Court Submission.* The remaining document—Document 9 in the attached index—is a classified 2002 submission to the Foreign Intelligence Surveillance Court (“FISC”). The submission is addressed to Judge Colleen Kollar-Kotelly, then the presiding judge of the FISC, and signed by a senior OLC attorney. It was provided to Judge Kollar-Kotelly to read, although not left in her possession. This is the sole document withheld by OLC only pursuant to

Exemptions One and Three, as it is not subject to the privileges discussed above. An unclassified attachment to this submission was released in full. I have been informed that a full classification review of Document 9 has been completed, and that the document may now be released to ACLU in less-redacted form. See Document 9, Letter from John Yoo to Judge Colleen Kollar-Kotelly (May 17, 2002), attached hereto as Exhibit G.

Withholdings Pursuant to Exemption Five

27. The ten OLC legal advice memoranda and one cover memorandum—together, Documents 1-7, the redacted portions of Documents 8 and 10, NSD 9, and NSD 36—are protected by the deliberative process privilege because they are confidential, pre-decisional, and deliberative. As legal advice, these documents are (a) pre-decisional, *i.e.*, were prepared in advance of Executive Branch decisionmaking; and (b) deliberative, *i.e.*, consist of advice to Executive Branch officials in connection with that decisionmaking. Consequently, these documents fall squarely within the protection of the deliberative process privilege. Compelled disclosure of these documents would undermine the deliberative processes of the Government and chill the candid and frank communications necessary for effective governmental decisionmaking.

28. In addition, these eleven documents withheld in full or in part contain communications protected by the attorney-client privilege. The responsive documents (a) contain confidential legal advice provided to OLC's Executive Branch clients; and (b) reflect confidential communications between OLC and Executive Branch clients made for the purpose of seeking and providing that legal advice. These documents thus fall squarely within the attorney-client privilege. The foregoing considerations regarding the need for confidential

deliberations are particularly compelling in the context of the seeking of legal advice by Executive Branch clients, and the provision of that legal advice by OLC.

Withholdings Pursuant to Exemptions One and Three

29. In connection with seeking advice from OLC, OLC's Executive Branch clients sometimes provide OLC with classified information or other information specifically protected from disclosure under FOIA by statute. OLC does not have original classification authority, but when it receives or makes use of classified information provided to it by its clients, OLC is required to mark and treat that information as derivatively classified to the same extent as its clients have identified such information as classified. Accordingly, all classified information in OLC's possession or incorporated into its products has been classified by another agency or component with original classifying authority.

30. I am familiar with the documents marked classified that are at issue in this case. As identified in the attached index, Documents 2-6 and 8-10 are marked as classified, as are NSD 9 and NSD 36. These documents are marked as classified because they contain information OLC received from other components or agencies that was marked as classified. OLC has also been informed by the relevant entities that information contained in these documents is protected from disclosure under FOIA by statute.

31. Accordingly, OLC is also withholding these documents in part pursuant to Exemptions One and Three. Exemption One, 5 U.S.C. § 552(b)(1), exempts documents classified in the interest of national defense or foreign policy pursuant to an Executive Order from disclosure under FOIA. Exemption Three, 5 U.S.C. § 552(b)(3), exempts documents "specifically exempted from disclosure by statute" from disclosure under FOIA. The application of these exemptions to these documents is addressed in other declarations being filed in

connection with this motion. *See* Declarations of David Sherman (addressing OLC Documents 2, 3, 4, 6, 8, and 9, and NSD 36), David M. Hardy (addressing OLC Documents 5 and 6, and NSD 9), and Antoinette B. Shiner (addressing OLC Document 5). The FBI has also asserted Exemptions Six and Seven over portions of OLC Documents 5 and 6, as described more fully in the Declaration of David M. Hardy.

Segregability, Adoption, and Waiver

32. I have personally reviewed each of the responsive documents that OLC withheld in whole or in part to determine whether any withheld portion or portions could be released without divulging information protected by one or more of the applicable FOIA exemptions. None of the withheld documents or redacted portions of produced documents contain reasonably segregable, nonexempt information.

33. To my knowledge, none of the withheld documents or redacted portions of produced documents have ever been publicly adopted or incorporated by reference by any policymaker as a basis for a policy decision.

34. To my knowledge, none of the withheld documents or redacted portions of produced documents have been previously publicly disclosed. In addition, I am not aware of any public statements by government officials that could constitute waiver of the privileges applicable to the withheld documents or redacted portions of produced documents

Discretionary Release

35. None of the withheld documents or redacted portions of produced documents is appropriate for discretionary release.

* * * * *

36. In conclusion, I respectfully submit that, except for Document 9, all of the withheld responsive documents or redacted portions of documents described herein are covered by the deliberative process privilege and/or the attorney-client privilege. Accordingly, the withheld documents and portions of documents fall squarely within Exemption Five. The compelled disclosure of these documents would harm the deliberative processes of the government and would disrupt the attorney-client relationship between OLC and its clients throughout the Executive Branch.

I declare under penalty of perjury that the foregoing is true and correct.

Executed: February 26, 2016, Washington, D.C.



PAUL P. COLBORN

Office of Legal Counsel (“OLC”)**Index of withheld records***ACLU et al. v. NSA et al.*, No. 13 Civ. 9198 (AT)

Doc. No.	Date	To	From	Description	Exemptions
Withheld in Full					
1	May 1984	The Attorney General	Theodore B. Olson, Assistant Attorney General (AAG), OLC	Cover memorandum for Document 2	(b)(5) deliberative process privilege (DP), attorney-client privilege (AC)
2	May 1984	The Attorney General	Olson	Legal advice memorandum discussing E.O. 12333 and addressing legal issues relating to certain surveillance activities	(b)(1); (b)(3), 50 U.S.C. § 3024(i)(1); (b)(5) DP, AC
3	September 2001	Deputy White House Counsel	John C. Yoo, Deputy Assistant Attorney General (DAAG), OLC	Legal advice memorandum regarding contemplated intelligence activities discussing, among other things, legal issues pertaining to surveillance under E.O. 12333	(b)(1); (b)(3), 50 U.S.C. § 3024(i)(1); (b)(5) DP, AC
4	October 2001	The Counsel to the President	Yoo	Legal advice memorandum regarding contemplated intelligence activities discussing, among other things, legal issues pertaining to surveillance under E.O. 12333	(b)(1); (b)(3), 50 U.S.C. § 3024(i)(1); (b)(5), DP, AC
5	April 2002	Counsel for Intelligence Policy	Yoo	Legal advice memorandum discussing, among other things, legal issues pertaining to surveillance under E.O. 12333	(b)(1); (b)(3), 50 U.S.C. § 3024(i)(1); (b)(5) DP, AC; (b)(7)(E)

Doc. No.	Date	To	From	Description	Exemptions
6	May 2003	The Deputy Attorney General	Yoo	Legal advice memorandum regarding contemplated intelligence activities discussing, among other things, legal issues pertaining to surveillance under E.O. 12333	(b)(1); (b)(3), 50 U.S.C. § 3024(i)(1); (b)(5) DP, AC; (b)(6); (b)(7)(A); (b)(7)(C); (b)(7)(D); (b)(7)(E);
7	May 2004	The Deputy Attorney General and Counsel for Intelligence Policy	Jack L. Goldsmith III, AAG, OLC	Legal advice memorandum discussing, among other things, legal issues pertaining to surveillance under E.O. 12333	(b)(5) DP, AC
Withheld in Part					
8	November 2, 2001	The Attorney General	Yoo	Legal advice memorandum discussing, among other things, legal issues pertaining to surveillance under E.O. 12333	(b)(1); (b)(3), 50 U.S.C. § 402 note, 50 U.S.C. § 3024(i)(1); (b)(5) DP, AC
9	May 2002	Judge Colleen Kollar-Kotelly, U.S. District Court for the District of Columbia	Yoo	Submission to Foreign Intelligence Surveillance Court discussing, among other things, legal issues pertaining to surveillance under E.O. 12333 (Attachment was released in full)	(b)(1); (b)(3), 50 U.S.C. § 402 note, 50 U.S.C. § 3024(i)(1)
10	May 6, 2004	The Attorney General	Goldsmith	Legal advice memorandum discussing, among other things, legal issues pertaining to surveillance under E.O. 12333	(b)(1); (b)(3), 50 U.S.C. § 402 note, 50 U.S.C. § 3024(i)(1); (b)(5) DP, AC



U.S. Department of Justice

Office of Legal Counsel

Washington, D.C. 20530

September 22, 2014

Alexander Abdo, Esq.
American Civil Liberties Union Foundation
125 Broad Street—18th Floor
New York, NY 10004

Re: *ACLU et ano v. NSA et al.*, No. 13-9198 (S.D.N.Y.); OLC FOIA No. FY13-051

Dear Mr. Abdo:

This letter responds to your May 13, 2013 Freedom of Information Act (“FOIA”) request to the Office of Legal Counsel (“OLC”) that is the subject of the above-captioned litigation. On July 10, 2013, you agreed to narrow your request to:

- 1) All OLC final legal advice concerning Executive Order 12333 or its implementing regulations with respect to electronic surveillance by the United States Government of communications of United States persons, regardless of whether the United States person is the target of the electronic surveillance or is in the United States at the time of the electronic surveillance. For purposes of this request, “electronic surveillance” and “United States person” have the meaning given in Executive Order 12333; and
- 2) All OLC final legal advice concerning the meaning of the terms “collection,” “acquisition,” and “interception” as used in Executive Order 12333 or its implementing regulations with respect to electronic surveillance by the United States Government of communications of United States persons. For purposes of this request, “electronic surveillance” has the meaning given in Executive Order 12333.

Pursuant to paragraph two of the May 9, 2014 Stipulation and Order Regarding Document Searches, and the parties’ Joint Scheduling Letter of June 20, 2014, we have completed our search of OLC’s files for records that are responsive to your request as narrowed, and have identified ten responsive documents.

Of these ten records, we are enclosing three records that contain redactions made pursuant to FOIA Exemptions One and Three, 5 U.S.C. § 552(b)(1), (3). The redacted portions are classified and specifically exempted from disclosure by 50 U.S.C. § 402 note and 50 U.S.C. § 3024(i)(1). Two of the three documents additionally contain redactions made pursuant to Exemption Five, 5 U.S.C. § 552(b)(5), because the material is protected by the deliberative process and attorney-client privileges.

We are withholding the remaining seven records in full under Exemption Five because they all are protected by the deliberative process and attorney-client privileges. Two of those documents also are protected by the presidential communications privilege, and six of the seven documents are

JA260

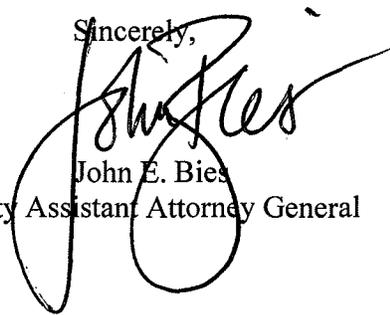
being withheld under Exemption One because they are classified. The classified documents may also be exempt under Exemption Three. We have determined that none of the withheld material is appropriate for discretionary release.

We are withholding these records in full today because they are currently classified, protected by statute, and privileged. As you are aware, the government is engaged in an ongoing large-scale, multi-agency review to determine whether additional information regarding its surveillance activities can be declassified and released consistent with national security. It is possible that in the future some of the responsive withheld records may, as part of these separate and ongoing efforts, be reviewed for possible declassification and discretionary release. In the event this separate review process results in the declassification of any portion of any of the responsive records withheld in full and the determination that the declassified portions are appropriate for discretionary release during the pendency of the litigation regarding this request, we will provide any such portions of the record to you at that time.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. *See* 5 U.S.C. § 552(c). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

Although your request is the subject of ongoing litigation, and administrative appeals are not ordinarily acted upon in such situations, I am required by statute and regulation to inform you that you have the right to file an administrative appeal. You must submit any administrative appeal within 60 days of the date of this letter by mail to the Office of Information Policy, United States Department of Justice, 1425 New York Avenue, N.W., Suite 11050, Washington, D.C. 20530; by fax at (202) 514-1009; or through OIP's e-portal at <http://www.justice.gov/oip/oip-request.html>. Both the letter and the envelope, or the fax, should be clearly marked "Freedom of Information Act Appeal."

Sincerely,



John E. Bies

Deputy Assistant Attorney General

cc: Jean-David Barnea
Assistant United States Attorney
Southern District of New York

David Jones
Assistant United States Attorney
Southern District of New York

Enclosures



U.S. Department of Justice

Office of Legal Counsel

Office of the Deputy Assistant Attorney General

Washington, D.C. 20530

November 2, 2001

MEMORANDUM FOR THE ATTORNEY GENERAL

From: John C. Yoo
Deputy Assistant Attorney General

b1, b3, b5

b1, b3, b5

b1, b3, b5

~~TOP SECRET~~^{b1, b3} / ~~SI/ORG/NOFORN~~

JA262

OLC 001

Pages 2-6
Withheld in Full

~~TOP SECRET~~^{b1, b3} /SI/OC/N/NOFORN
b1, b3, b5

b1, b3, b5

FISA only provides a safe harbor
for electronic surveillance, and cannot restrict the President's ability to engage in warrantless searches
that protect the national security.

b1, b3, b5

7

Page 8

Withheld in Full

~~TOP SECRET~~ b1, b3 ~~NOFORN~~

FISA purports to be the exclusive statutory means for conducting electronic surveillance for foreign intelligence.

b1, b3, b5

Such a reading of FISA would be an unconstitutional infringement on the President's Article II authorities.

b1, b3, b5

b1, b3, b5

Pages 10-11
Withheld in Full

~~TOP SECRET~~ b1, b3 ~~TOP SECRET~~
b1, b3, b5

Thus, unless Congress made a clear statement in FISA that it sought to restrict presidential authority to conduct warrantless searches in the national security area - which it has not - then the statute must be construed to avoid such a reading

b1, b3, b5

b1, b3, b5

Pages 13-16
Withheld in Full

~~TOP SECRET~~ b1, b3 ~~SIORCONNOFORN~~

b1, b3, b5

we do not believe that Congress may restrict the President's inherent constitutional powers, which allow him to gather intelligence necessary to defend the nation from direct attack.

intelligence gathering in direct support of military operations does not trigger constitutional rights against illegal searches and seizures.

b1, b3, b5

Page 18
Withheld in Full

JA271

OLC 010

~~TOP SECRET~~ b1, b3 ~~SI/ORCON/NOFORN~~
b1, b3, b5

b1, b3, b5

b1, b3, b5

A warrantless search can be constitutional "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable."

b1, b3, b5

Page 20
Withheld in Full

~~TOP SECRET~~ b1, b3 ~~NOFORN~~

b1, b3, b5

...governmental interest is more compelling than the security of the Nation." *Haig v. Agee*, 453 U.S. 280, 307 (1981).

b1, b3, b5

b1, b3, b5

Pages 22-24
Withheld in Full



~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

U.S. Department of Justice

Office of Legal Counsel

Office of the Assistant Attorney General

Washington, D.C. 20530

May 6, 2004

MEMORANDUM FOR THE ATTORNEY GENERAL

Re: Review of the Legality of the STELLAR WIND Program (TS//SI- STELW//NF)

BACKGROUND

- A. September 11, 2001 5
- B. Initiation of STELLAR WIND 6
- C. Reauthorizations and the Reauthorization Process 8
- D. Modifications to STELLAR WIND Authority 9
- E. Operation of the Program and the Modifications of March 2004 11
- F. Prior Opinions of this Office 17

ANALYSIS

- I. STELLAR WIND Under Executive Order 12,333 18
- II. Content Collection – Statutory Analysis 19
 - A. Prior Opinions of this Office – Constitutional Avoidance 22
 - B. Analysis of STELLAR WIND Under FISA Must Take Into Account the September 2001 Congressional Authorization for Use of Military Force 29
 - 1. The Congressional Authorization provides express authority for STELLAR WIND content collection 29
 - 2. At a minimum, the Congressional Authorization bolsters the case for applying the canon of constitutional avoidance 35
 - C. If FISA Purported To Prohibit Targeted, Wartime Surveillance Against the Enemy Under STELLAR WIND, It Would Be Unconstitutional As Applied 37
 - 1. Even in peacetime, absent congressional action, the President has inherent constitutional authority, consistent with the Fourth Amendment, to order warrantless foreign intelligence surveillance 37
 - 2. FISA is unconstitutional as applied in this context 43
 - a. Even outside the context of wartime surveillance of the enemy, the scope of Congress’s power to restrict the President’s inherent authority to conduct foreign intelligence surveillance is unclear 44
 - b. In the narrow context of interception of enemy communications in the midst of an armed conflict, FISA is unconstitutional as applied 51

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

Derived from: “Presidential Authorization for Specified Electronic Surveillance Activities During a Limited Period to Detect and Prevent Acts of Terrorism Within the United States,” dated Oct. 4, 2001, and subsequent related Presidential authorizations

Declassify only upon determination by the President

TOP SECRET////COMINT-STELLAR WIND//NOFORN

3.	 	74
III.	Telephony Dialing-Type Meta Data Collection – Statutory Analysis	81
A.	 	83
B.	 	86
C.	 	89
IV.	 	96
	 	96
	 	98
	 	99
	 	100
V.	STELLAR WIND Under the Fourth Amendment	100
A.	STELLAR WIND Content Interceptions Are Reasonable Under Balancing-of-Interests Analysis	101
B.	Acquisition of Meta Data Does Not Implicate the Fourth Amendment	106
	CONCLUSION	108

You have asked this Office to undertake a thorough reexamination of the STELLAR WIND program as it is currently operated to confirm that the actions that the President has directed the Department of Defense to undertake through the National Security Agency (NSA) are lawful. STELLAR WIND is a highly classified and strictly compartmented program of electronic surveillance within the United States that President Bush directed the Department of Defense to undertake on October 4, 2001 in response to the attacks of September 11, 2001. Specifically, the program is designed to counter the threat of further terrorist attacks on the territorial United States by detecting communications that will disclose terrorist operatives, terrorist plans, or other information that can enable the disruption of such attacks, particularly the identification of al Qaeda operatives within the United States. The President's initial directive to the Secretary of Defense authorized the STELLAR WIND program for 30 days. Since then, the President has periodically (roughly every 30 to 45 days) reauthorized the program.

(TS//SI//COMINT//STLW//NF)

After describing the initiation of STELLAR WIND, modifications to the program, and its current operation, including the periodic reauthorizations by the President, this memorandum provides a legal analysis of the program in four parts. In Part I, we briefly examine STELLAR WIND under Executive Order 12,333, 46 Fed. Reg. 59, 941 (Dec. 4, 1981), the Executive Order governing the responsibilities and conduct of various entities in the intelligence community.

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

TOP SECRET////COMINT-STELLAR WIND//NOFORN

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

In Part II, we address the statutory framework that governs the interception of communications in the United States and its application to the first of the three major parts of the STELLAR WIND program – that is, targeted interception of the content of international communications involving suspected terrorists. Specifically, we address the Foreign Intelligence Surveillance Act (FISA), as amended, 50 U.S.C. §§ 1801-1862 (2000 & Supp. I 2001), and relevant related provisions in Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, 18 U.S.C. §§ 2510-2521 (“Title III”) (2000 & Supp. I 2001).¹

[REDACTED] we turn to a new analysis of STELLAR WIND in relation to FISA based on the recognition that a proper legal review should not examine FISA in isolation. Rather, in the context of STELLAR WIND collection in the ongoing conflict with al Qaeda, the restrictions in FISA must be read in light of the express authorization enacted by Congress on September 18, 2001 providing the President authority “to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks” of September 11. Authorization for Use of Military Force, Pub. L. No. 107-40, § 2(a), 115 Stat. 224, 224 (Sept. 18, 2001) (reported as a note to 50 U.S.C.A. § 1541) (“Congressional Authorization”). The Congressional Authorization is significant for our analysis in two respects. First, it is properly understood as an express authorization for surveillance activities – including the content collection undertaken as part of STELLAR WIND – targeted against al Qaeda and affiliated organizations that come within its terms. Second, even if it did not provide express authority for the targeted content collection undertaken as part of STELLAR WIND, at a minimum the Congressional Authorization creates sufficient ambiguity concerning the application of FISA in this context that the canon of constitutional avoidance can properly be invoked to construe the Congressional Authorization to overcome restrictions in FISA in this context.

(TS//SI-STLW//NF)

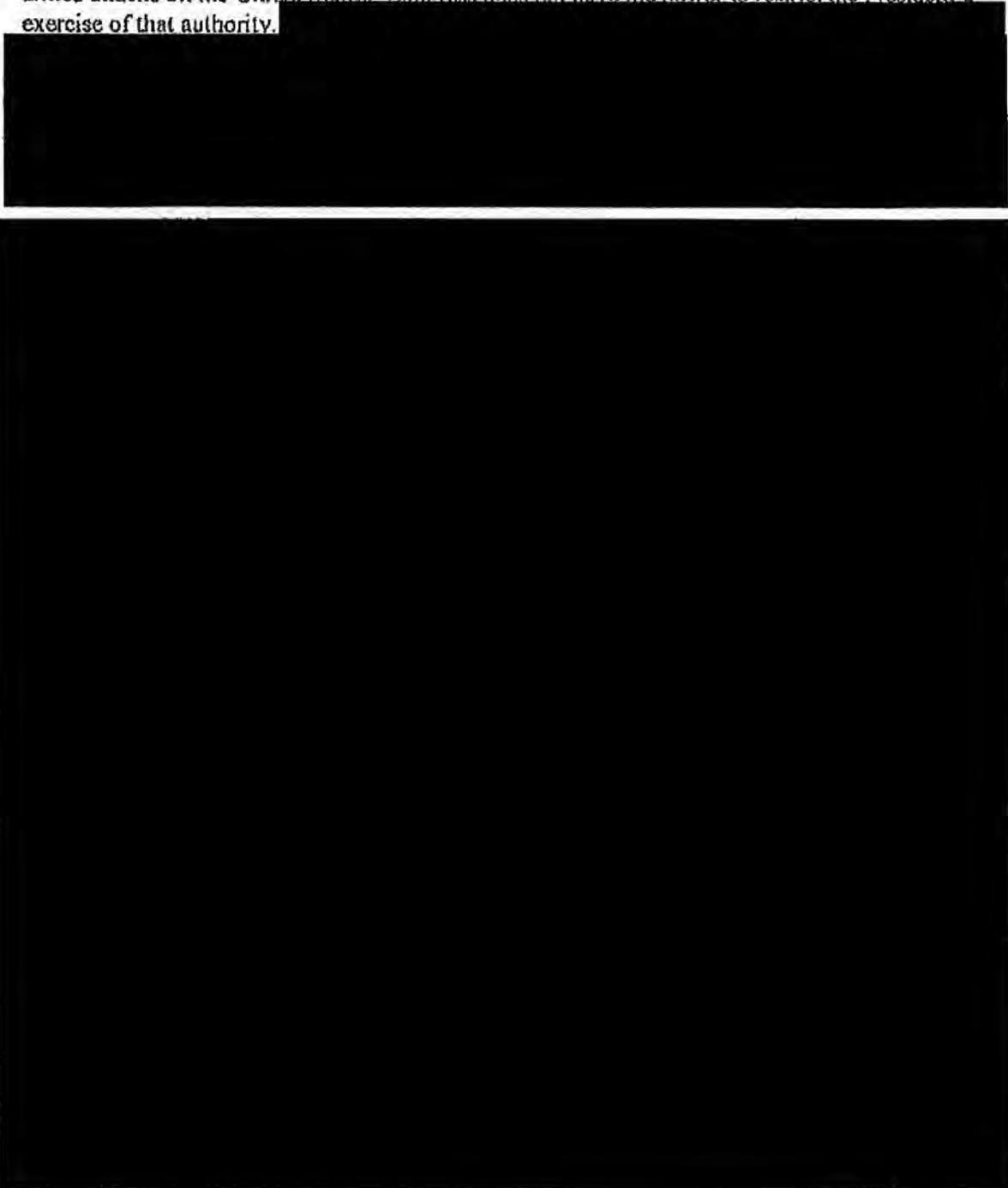
[REDACTED] We conclude that in the circumstances of the current armed conflict with al Qaeda, the restrictions set out in FISA, as applied to targeted efforts to intercept the communications of the enemy in order to prevent further armed attacks on the United States, would be an unconstitutional infringement

¹ Unless otherwise noted, all United States Code citations in this memorandum are to the 2000 edition. (U)

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

~~TOP SECRET// [REDACTED]//COMINT- STELLAR WIND [REDACTED]//NOFORN~~

on the constitutionally assigned powers of the President. The President has inherent constitutional authority as Commander in Chief and sole organ for the nation in foreign affairs to conduct warrantless surveillance of enemy forces for intelligence purposes to detect and disrupt armed attacks on the United States. Congress does not have the power to restrict the President's exercise of that authority.



~~TOP SECRET// [REDACTED]//COMINT- STELLAR WIND [REDACTED]//NOFORN~~

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

Finally, in Part V, we examine STELLAR WIND content collection and meta data collection (for both telephony and e-mail) under the requirements of the Fourth Amendment. Although no statutory requirements prevent the President from conducting surveillance under STELLAR WIND, electronic surveillance under STELLAR WIND must still comply with the requirements of the Fourth Amendment. We reaffirm our conclusions (i) that as to content collection, STELLAR WIND activities come within an exception to the Warrant Clause and satisfy the Fourth Amendment's requirement of reasonableness, and (ii) that meta data collection does not implicate the Fourth Amendment. The activities authorized under STELLAR WIND are thus constitutionally permissible. (TS//SI- STLW//NF)

BACKGROUND (U)

A. September 11, 2001 (U)

On September 11, 2001, the al Qaeda terrorist network launched a set of coordinated attacks along the East Coast of the United States. Four commercial airliners, each apparently carefully selected because it was fully loaded with fuel for a transcontinental flight, were hijacked by al Qaeda operatives. Two were targeted at the Nation's financial center in New York and were deliberately flown into the two towers of the World Trade Center. The third was targeted at the headquarters of the Nation's armed forces, the Pentagon. The fourth was apparently headed toward Washington, D.C., when passengers struggled with the hijackers and the plane crashed in Pennsylvania. Subsequent debriefings of captured al Qaeda operatives have confirmed that the intended target of this plane was either the White House or the Capitol building, which suggests that its intended mission was a decapitation strike – an attempt to eliminate critical governmental leaders by killing either the President or a large percentage of the members of the Legislative Branch. These attacks resulted in approximately 3,000 deaths – the highest single-day death toll from foreign hostile action in the Nation's history. They also shut down air travel in the United States for several days, closed the New York Stock Exchange for days, and caused billions of dollars in damage to the economy. (U)

On September 14, 2001, the President declared a national emergency "by reason of the terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and the continuing and immediate threat of further attacks on the United States." Proclamation No. 7463, 66 Fed. Reg. 48,199 (Sept. 14, 2001). The United States also launched a massive military response, both at home and abroad. In the United States, combat air patrols were immediately established over major metropolitan areas and were maintained 24 hours a day until April 2002.² The United States also immediately began plans for a military response directed at al Qaeda's base of operations in Afghanistan. On September 14, 2001, both houses of Congress passed a joint resolution authorizing the President "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks" of September 11. Congressional Authorization § 2(a). Congress also expressly

(S)

5

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

~~TOP SECRET//COMINT-**[REDACTED]** STELLAR WIND//NOFORN~~

acknowledged that the attacks rendered it "necessary and appropriate" for the United States to exercise its right "to protect United States citizens both at home and abroad," and acknowledged in particular that the "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States." *Id.* pmb1. Acting under his constitutional authority as Commander in Chief, and with the support of Congress, the President dispatched forces to Afghanistan and, with the cooperation of the Northern Alliance, toppled the Taliban regime from power. Military operations to seek out resurgent elements of the Taliban regime and al Qaeda fighters continue in Afghanistan to this day. *See, e.g.,* Mike Wise and Josh White, *Ex-NFL Player Tillman Killed in Combat*, Wash. Post, Apr. 24, 2004, at A1 (noting that "there are still more than 10,000 U.S. troops in the country and fighting continues against remnants of the Taliban and al Qaeda"). (S)

As the President made explicit in his Military Order of November 13, 2001, authorizing the use of military commissions to try terrorists, the attacks of September 11 "created a state of armed conflict." Military Order, § 1(a), 66 Fed. Reg. 57,833, 57,833 (Nov. 13, 2001); *see also* Memorandum for Alberto R. Gonzales, Counsel to the President, from Patrick F. Philbin, Deputy Assistant Attorney General, Office of Legal Counsel, *Re: Legality of the Use of Military Commissions To Try Terrorists* 22-28 (Nov. 6, 2001) (concluding that attacks established a state of armed conflict permitting invocation of the laws of war). Indeed, shortly after the attacks NATO took the unprecedented step of invoking article 5 of the North Atlantic Treaty, which provides that an "armed attack against one or more of [the parties] shall be considered an attack against them all." North Atlantic Treaty, Apr. 4, 1949, art. 5, 63 Stat. 2241, 2244, 34 U.N.T.S. 243, 246; *see also* Statement by NATO Secretary General Lord Robertson (Oct. 2, 2001), available at <http://www.nato.int/docu/speech/2001/s011002a.htm> ("[I]t has now been determined that the attack against the United States on 11 September was directed from abroad and shall therefore be regarded as an action covered by Article 5 of the Washington Treaty . . ."). The President also determined in his Military Order that al Qaeda terrorists "possess both the capability and the intention to undertake further terrorist attacks against the United States that, if not detected and prevented, will cause mass deaths, mass injuries, and massive destruction of property, and may place at risk the continuity of the operations of the United States Government," and concluded that "an extraordinary emergency exists for national defense purposes." Military Order, § 1(c), (g), 66 Fed. Reg. at 57,833-34. (U)

B. Initiation of STELLAR WIND (~~TS//SI-STLW//NF~~)

Against this unfolding background of events in the fall of 2001, there was substantial concern that al Qaeda was preparing a further attack within the United States. Al Qaeda had demonstrated its ability to infiltrate agents into the United States undetected and have them carry out devastating attacks, and it was suspected that further agents were likely already in position within the Nation's borders. Indeed, to this day finding al Qaeda sleeper agents in the United States remains one of the top concerns in the war on terrorism. As FBI Director Mueller recently stated in classified testimony before Congress, "[t]he task of finding and neutralizing al-Qa'ida operatives that have already entered the U.S. and have established themselves in American society is one of our most serious intelligence and law enforcement challenges." Testimony of

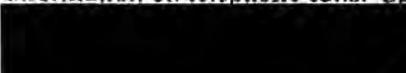
~~TOP SECRET//COMINT-**[REDACTED]** STELLAR WIND//NOFORN~~

~~TOP SECRET//COMINT--STELLAR WIND-//NOFORN~~

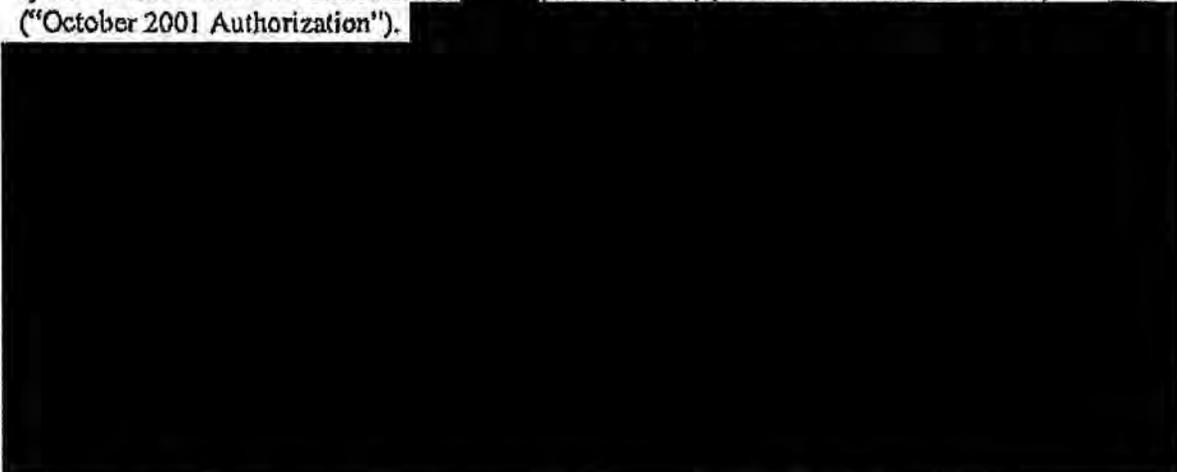
Robert S. Mueller, III, Director, FBI, Before the Senate Select Comm. on Intelligence 5 (Feb. 24, 2004) (S/ORCON,NF). (S//NF)

To counter that threat, on October 4, 2001, the President directed the Secretary of Defense to use the capabilities of the Department of Defense, in particular the National Security Agency (NSA), to undertake a program of electronic surveillance designed to 

 countering the threat of further al Qaeda attacks within the United States. This program is known by the code name "STELLAR WIND." The electronic surveillance activities that the President authorized under STELLAR WIND fall into two broad categories: (1) interception of the *content* of certain communications, and (2) collection of *header/router/addressing information* on communications, such as dialing number information on telephone calls. Specifically, 

 communications for which there was probable cause to believe that at least one party to the communication 

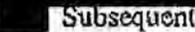
Presidential Authorization for Specified Electronic Surveillance Activities During a Limited Period to Detect and Prevent Acts of Terrorism Within the United States (Oct. 4, 2001) (TS//SI//COMINT//STLW/NF) ("October 2001 Authorization"). 



The President further directed that the Department of Defense should minimize the information collected concerning American citizens, consistent with the object of detecting and preventing terrorism. See October 2001 Authorization 

The October 4, 2001

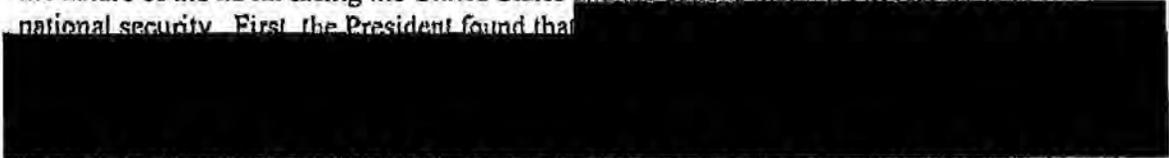
Presidential Authorization stated: 

 October 2001 Authorization  Subsequent Presidential Authorizations have repeated identical language. (TS//SI//STLW/NF)

~~TOP SECRET//COMINT--STELLAR WIND-//NOFORN~~

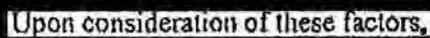
~~TOP SECRET//COMINT--STELLAR WIND-//NOFORN~~

The President based his decision to initiate the program on specific findings concerning the nature of the threat facing the United States and the actions that were necessary to protect national security. First, the President found that 



Second, the President noted that he had considered the magnitude and probability of deaths and destruction that could result from further terrorist attacks; the need to detect and prevent such attacks, particularly through effective electronic surveillance that could be initiated swiftly and with secrecy; the possible intrusion into the privacy of American citizens that might result from the electronic surveillance being authorized; the absence of more narrowly tailored means of obtaining the information that was the object of the surveillance; and the 



 Upon consideration of these factors, the President determined that  and that this emergency constitute  that supported conducting the described surveillance without resort to judicial warrants.  The President noted, however, that he intended to inform the appropriate members of the Senate and the House of Representatives as soon as that could be done consistent with national defense needs. 

(TS//SI-STLW//NF)

C. Reauthorizations and the Reauthorization Process (TS//SI-STLW//NF)

As noted above, the President's Authorization of October 4, 2001, was limited in duration and set its own expiration date for thirty days from the date on which it was signed. Since then, the STELLAR WIND program has been periodically reauthorized by the President, with each authorization lasting a defined time period, typically 30 to 45 days. The restriction of each authorization to a limited duration has ensured that the basic findings described above upon which the President assesses the need for the STELLAR WIND program are re-evaluated by the

³ We note that, in compliance with the President's instructions, the chairmen and ranking minority members of the House and Senate intelligence committees were briefed periodically on STELLAR WIND by the Director of the NSA in 2002 and 2003. 

~~TOP SECRET//COMINT--STELLAR WIND-//NOFORN~~

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

President and his senior advisors based on current information every time that the program is reauthorized. (TS//SI-STLW//NF)

The reauthorization process operates as follows. As the period of each reauthorization nears an end, the Director of Central Intelligence (DCI) prepares a memorandum for the President outlining selected current information concerning the continuing threat that al Qaeda poses for conducting attacks in the United States, as well as information describing the broader context of al Qaeda plans to attack U.S. interests around the world. Both the DCI and the Secretary of Defense review that memorandum and sign a recommendation that the President should reauthorize STELLAR WIND based on the continuing threat posed by potential terrorist attacks within the United States. That recommendation is then reviewed by this Office. Based upon the information provided in the recommendation, and also taking into account information available to the President from all sources, this Office assesses whether there is a sufficient factual basis demonstrating a threat of terrorist attacks in the United States for it to continue to be reasonable under the standards of the Fourth Amendment for the President to authorize the warrantless searches involved in STELLAR WIND. (The details of the constitutional analysis this Office has applied are reviewed in Part V of this memorandum.) As explained in more detail below, since the inception of STELLAR WIND, intelligence from various sources (particularly from interrogations of detained al Qaeda operatives) has provided a continuing flow of information indicating that al Qaeda has had, and continues to have, multiple redundant plans for executing further attacks within the United States. These strategies are at various stages of planning and execution, and some have been disrupted. They include plans for [REDACTED]

[REDACTED] After reviewing each of the proposed STELLAR WIND reauthorizations, this Office has advised you that the proposed reauthorization would satisfy relevant constitutional standards of reasonableness under the Fourth Amendment, as described in this Office's earlier memoranda. Based on that advice, you have approved as to form and legality each reauthorization to date, except for the Authorization of March 11, 2004 (discussed further below), and forwarded it to the President for his action. (TS//SI-STLW//NF)

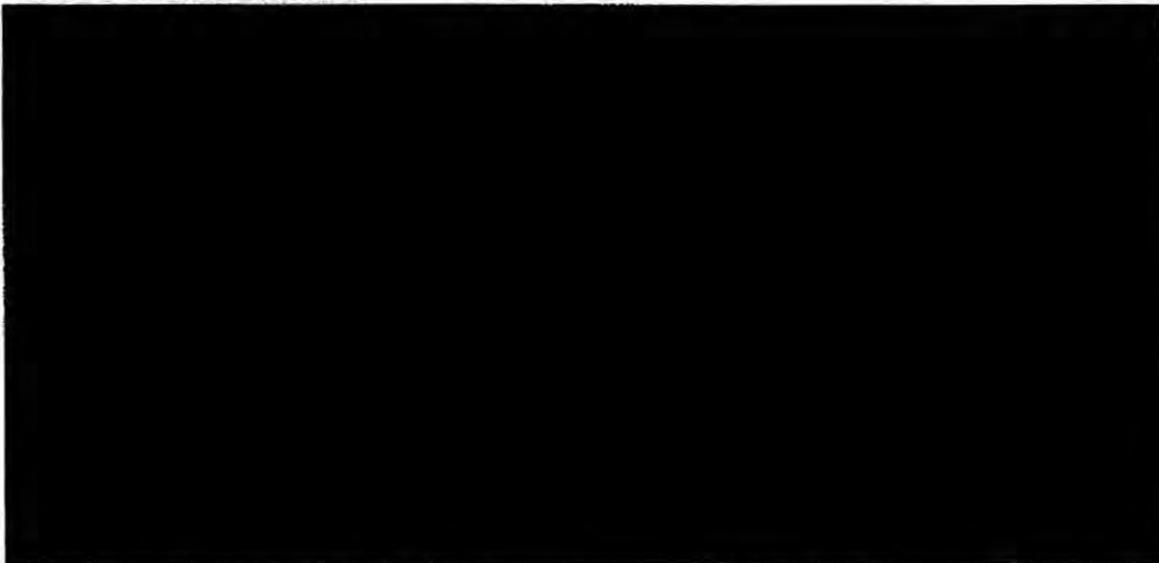
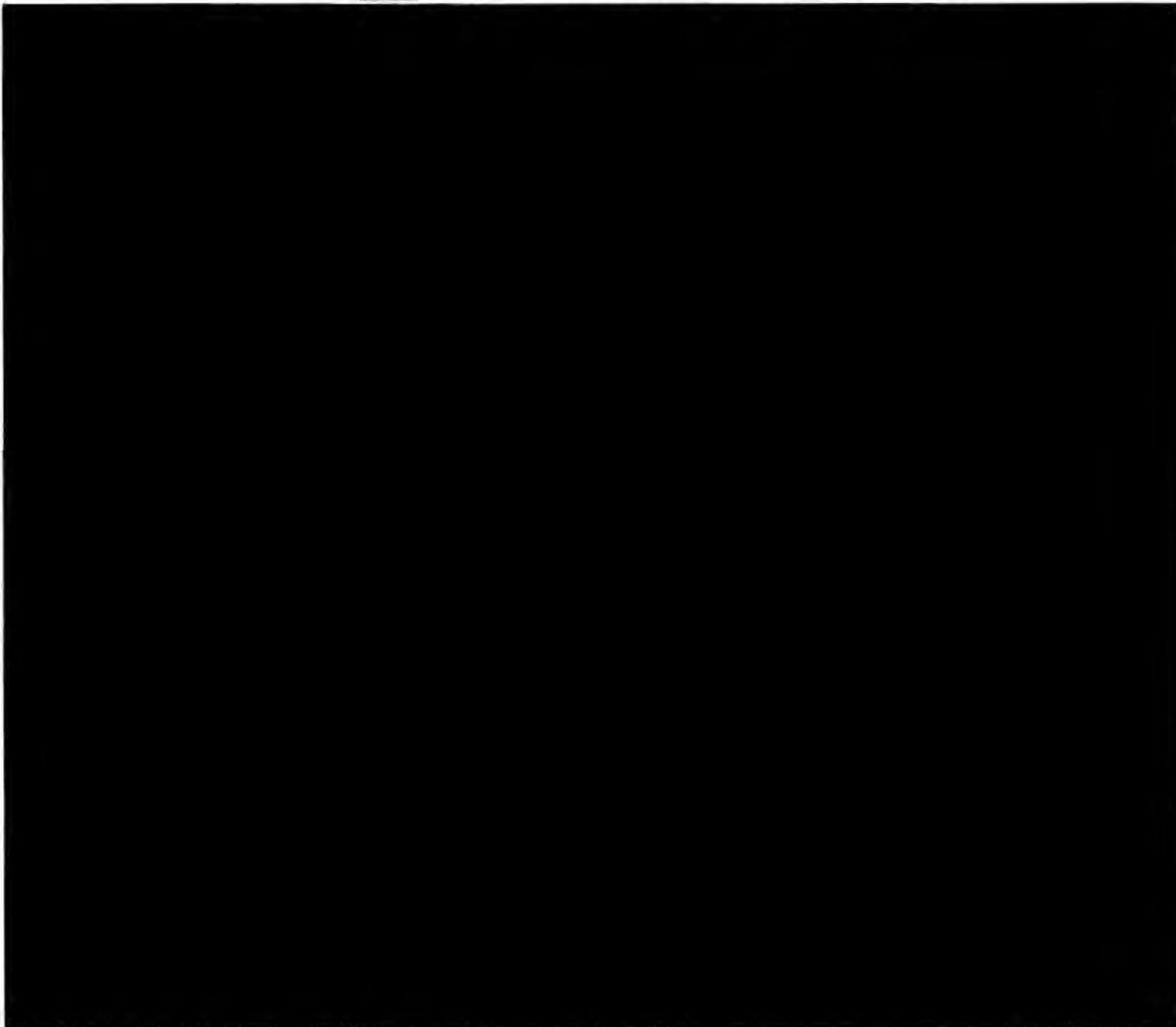
Each authorization also includes the instructions noted above to minimize the information collected concerning American citizens, consistent with the objective of detecting and preventing terrorism. [REDACTED] (TS//SI-STLW//NF)

D. Modifications to STELLAR WIND Authority (TS//SI-STLW//NF)

The scope of the authorization for electronic surveillance under STELLAR WIND has changed over time. The changes are most easily understood as being divided into two phases: (i) those that occurred before March 2004, and (ii) those that occurred in March [REDACTED] 2004. (TS//SI-STLW//NF)

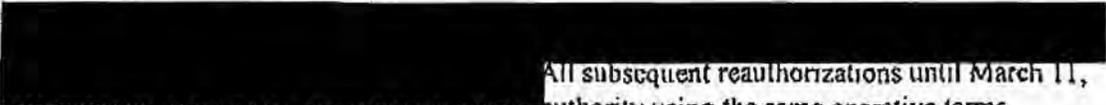
~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

~~TOP SECRET~~ [REDACTED] ~~COMINT-STAR WIND~~ [REDACTED] ~~NOFORN~~



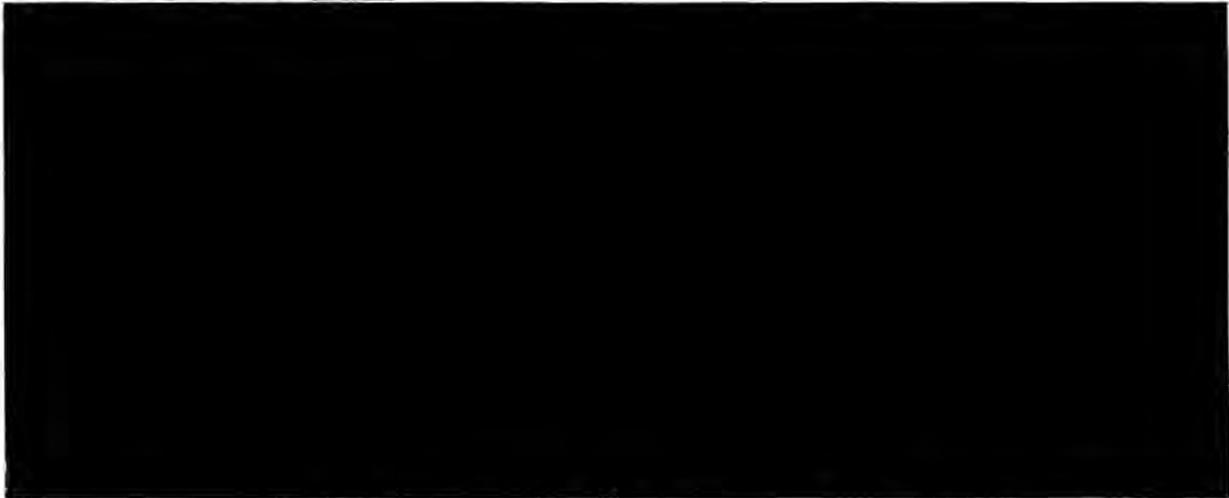
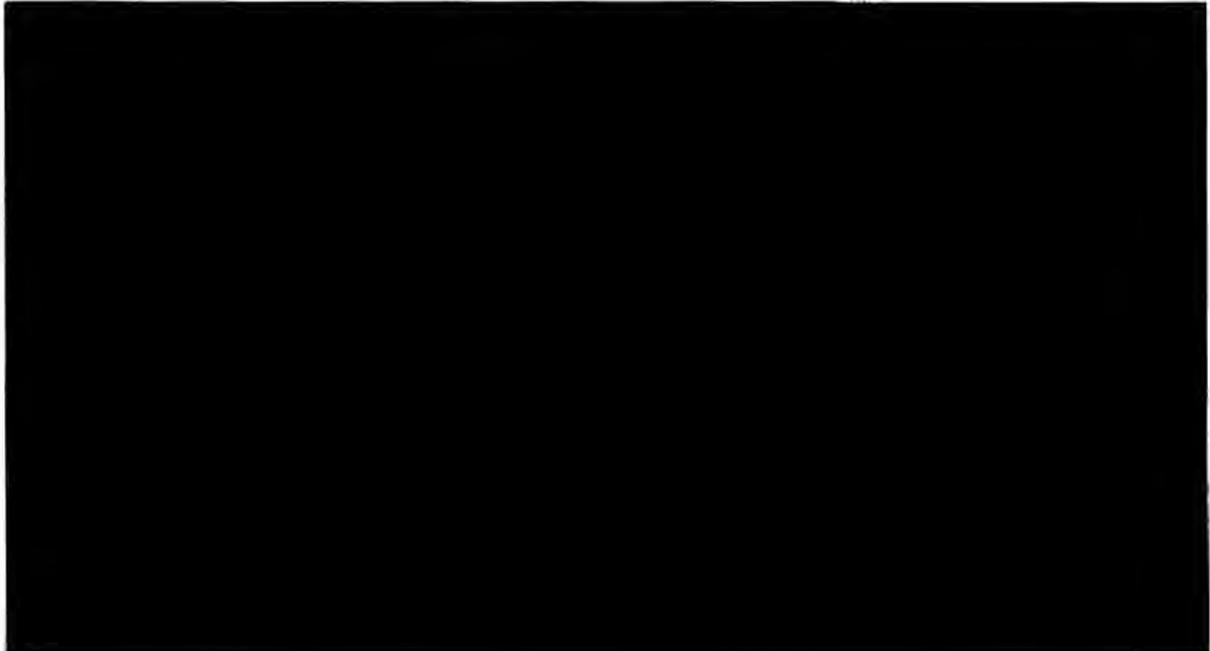
~~TOP SECRET~~ [REDACTED] ~~COMINT-STAR WIND~~ [REDACTED] ~~NOFORN~~

~~TOP SECRET//COMINT--STELLAR WIND-//NOFORN~~

 All subsequent reauthorizations until March 11, 2004 provided the Secretary of Defense with authority using the same operative terms. (TS//SI-STLW//NF)

E. Operation of the Program and the Modifications of March  2004
(TS//SI-STLW//NF)

A second, more substantial series of changes to STELLAR WIND took place in March  2004. To understand these changes, it is necessary to understand some background concerning how the NSA accomplishes the collection activity authorized under STELLAR WIND. (TS//SI-STLW//NF)



~~TOP SECRET//COMINT--STELLAR WIND-//NOFORN~~

Pages 12 – 14

Withheld in Full

TOP SECRET//~~COMINT~~-STELLAR WIND//NOFORN



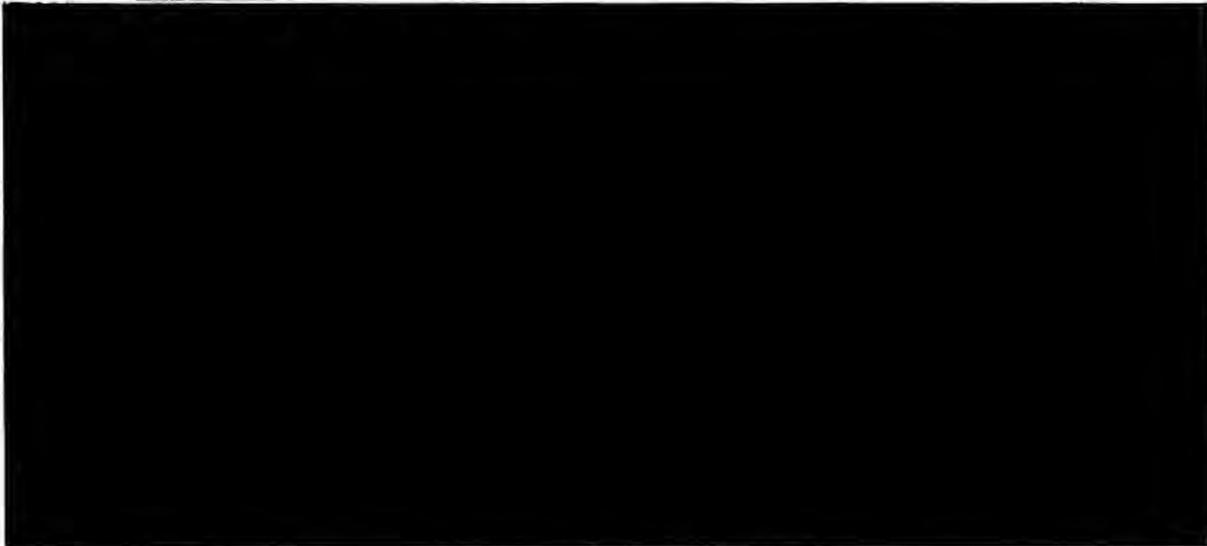
Third, the March 11, 2004 Authorization also makes clear that these changes are consistent with all past Authorizations



(TS//SI-STLW//NF)

Finally, the President, exercising his constitutional authority under Article II determined that the March 11, 2004 Authorization and all prior Authorizations were lawful exercises of the President's authority under Article II, including the Commander-in-Chief Clause.

(TS//SI-STLW//NF)



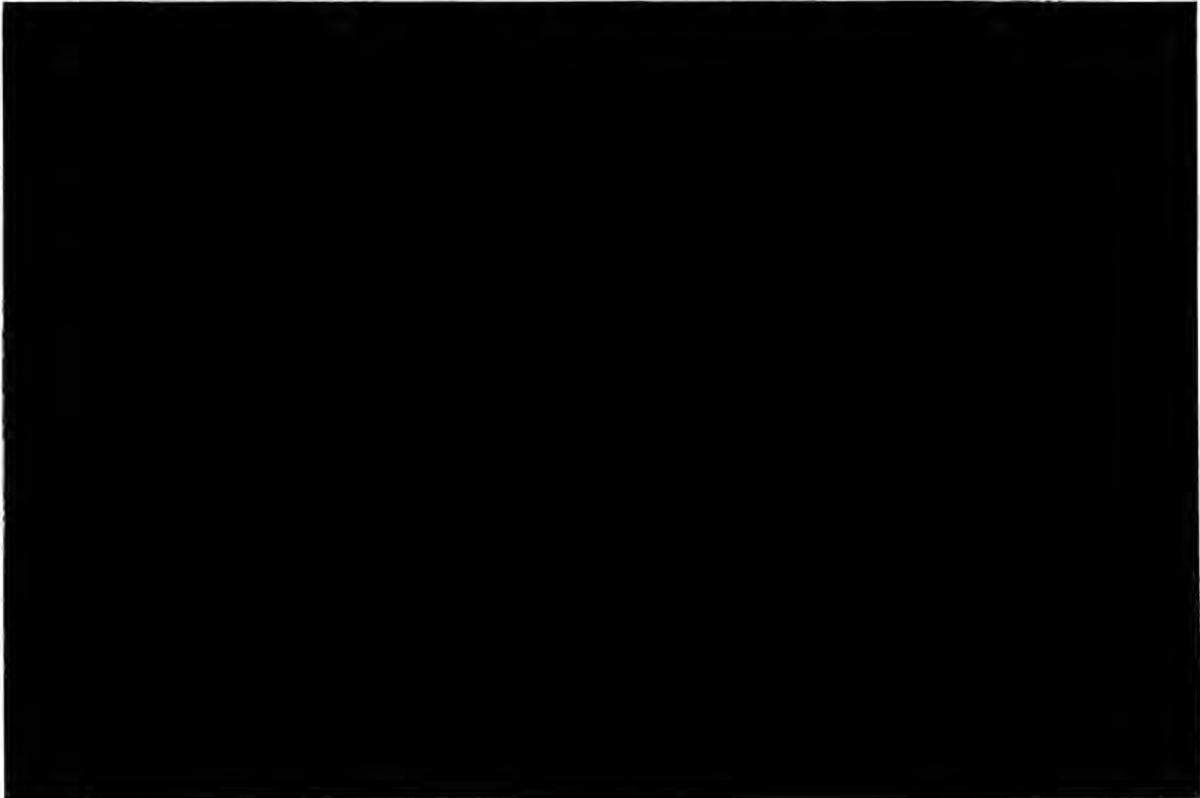
TOP SECRET//~~COMINT~~-STELLAR WIND//NOFORN

~~TOP SECRET~~ [REDACTED] ~~/COMINT- STELLAR WIND~~ [REDACTED] ~~/NOFORN~~

In the March 19, 2004 Modification, the President also clarified the scope of the authorization for intercepting the content of communications. He made clear that the Authorization applied where there were reasonable grounds to believe that a communicant was an agent of an international terrorist group [REDACTED]

March 19, 2004

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



This memorandum analyzes STELLAR WIND as it currently operates.¹¹ To summarize, that includes solely the following authorities:

- (1) the authority to intercept the content of international communications "for which, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are reasonable grounds to believe . . . [that] a party to such communication is a group engaged in international terrorism, or activities in preparation therefor, or any agent of such a group," as long as that



~~TOP SECRET~~ [REDACTED] ~~/COMINT- STELLAR WIND~~ [REDACTED] ~~/NOFORN~~

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

group is al Qaeda, an affiliate of al Qaeda or another international terrorist group that the President has determined both (a) is in armed conflict with the United States and (b) poses a threat of hostile action within the United States;¹²

(2)

[REDACTED]

(3)

[REDACTED]

F. Prior Opinions of this Office (U)

This Office has issued several opinions analyzing constitutional and other legal issues related to the STELLAR WIND program. On October 4, 2001 [REDACTED] we evaluated the legality of a hypothetical electronic surveillance program [REDACTED]

On November 2, 2001, we expressly examined the authorities granted by the President in the November 2, 2001 Authorization of STELLAR WIND and concluded that they were lawful. [REDACTED]

Finally, on October 11, 2002, we issued an opinion confirming the application of our prior analysis to the reauthorization of the program then pending, which was to continue the program until November 21, 2002. [REDACTED]

[REDACTED]

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

~~TOP SECRET//COMINT- STELLAR WIND~~ ~~NOFORN~~

[REDACTED]

You have asked us to undertake a thorough review of the current program to ensure that it is lawful. ~~(TS//SI- STELW//NF)~~

ANALYSIS (U)

- i. STELLAR WIND Under Executive Order 12,333 ~~(TS//SI- STELW//NF)~~

[REDACTED]

[REDACTED]

~~TOP SECRET//COMINT- STELLAR WIND~~ ~~NOFORN~~

~~TOP SECRET// [REDACTED] //COMINT- STELLAR WIND [REDACTED] //NOFORN~~

II. Content Collection ~ Statutory Analysis (~~TS//SI- STELW//NF~~)

In this Part, we turn to an analysis of STELLAR WIND content collection under relevant statutes regulating the government's interception of communications, specifically under the framework established by the Foreign Intelligence Surveillance Act and title III of the Omnibus Crime Control and Safe Streets Act of 1968. Generally speaking, FISA sets out several authorities for the government to use in gathering foreign intelligence (including authority to intercept communications, conduct physical searches, and install pen registers); establishes certain procedures that must be followed for these authorities to be used (procedures that usually involve applying for and obtaining an order from a special court); and, for some of these authorities, provides that the processes provided by FISA are the *exclusive* means for the government to engage in the activity described. Title III and related provisions codified in title 18 of the United States Code provide authorities for the use of electronic surveillance for law enforcement purposes. Because the statutory provisions governing the interception of the content of communications are different under both regimes from those governing the interception of dialing number/routing information, we analyze the authorities under STELLAR WIND that relate to collection of meta data separately in Parts III and IV. (~~TS//SI- STELW//NF~~)

Generally speaking, FISA provides what purports to be, according to the terms of the statute, the exclusive means for intercepting the content of communications in the United States for foreign intelligence purposes. Specifically, FISA sets out a definition of "electronic surveillance"¹⁵ – a definition that includes any interception in the United States of the contents of

¹⁵ FISA defines "[e]lectronic surveillance" as:

- (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

~~TOP SECRET// [REDACTED] //COMINT- STELLAR WIND [REDACTED] //NOFORN~~

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

a "wire communication" to or from a person in the United States – and provides specific procedures that must be followed for the government to engage in "electronic surveillance" as thus defined for foreign intelligence purposes. As a general matter, for electronic surveillance to be conducted, FISA requires that the Attorney General or Deputy Attorney General approve an application for an order that must be submitted to a special Article III court created by FISA – the Foreign Intelligence Surveillance Court (FISC). *See* 50 U.S.C. § 1804 (2000 & Supp. I 2001).¹⁶ The application for an order must demonstrate, among other things, that there is probable cause to believe that the target is a foreign power or an agent of a foreign power. *See id.* § 1805(a)(3)(A). It must also contain a certification from the Assistant to the President for National Security Affairs or an officer of the United States appointed by the President with the advice and consent of the Senate and having responsibilities in the area of national security or defense that the information sought is foreign intelligence information (as defined by FISA), that cannot reasonably be obtained by normal investigative means. *See id.* § 1804(a)(7). FISA further requires details about the methods that will be used to obtain the information and the particular facilities that will be the subject of the interception. *See id.* § 1804(a)(4), (a)(8).
(TS//SI-STLW//NF)

FISA expressly makes it a felony offense, punishable by up to 5 years in prison, for any person intentionally to conduct electronic surveillance under color of law except as provided by statute. *See* 50 U.S.C. § 1809.¹⁷ This provision is complemented by an interlocking provision in Title III – the portion of the criminal code that provides the mechanism for obtaining wire taps for law enforcement purposes. Section 2511 of title 18 makes it an offense, also punishable by up to 5 years in prison, for any person to intercept a communication except as specifically provided in that chapter. 18 U.S.C. § 2511(1)(a), (4)(a). One of the exceptions expressly provided is that it is not unlawful for "an officer, employee, or agent of the United States . . . to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act." *Id.* § 2511(2)(c) (emphasis added). On their face, these provisions make FISA, and the authorization process it requires, the exclusive lawful means for the Executive to engage in "electronic surveillance," as defined in the Act for foreign intelligence

of any party thereto, if such acquisition occurs in the United States . . . ;

(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) (2000 & Supp. I 2001). (TS//SI-STLW//NF)

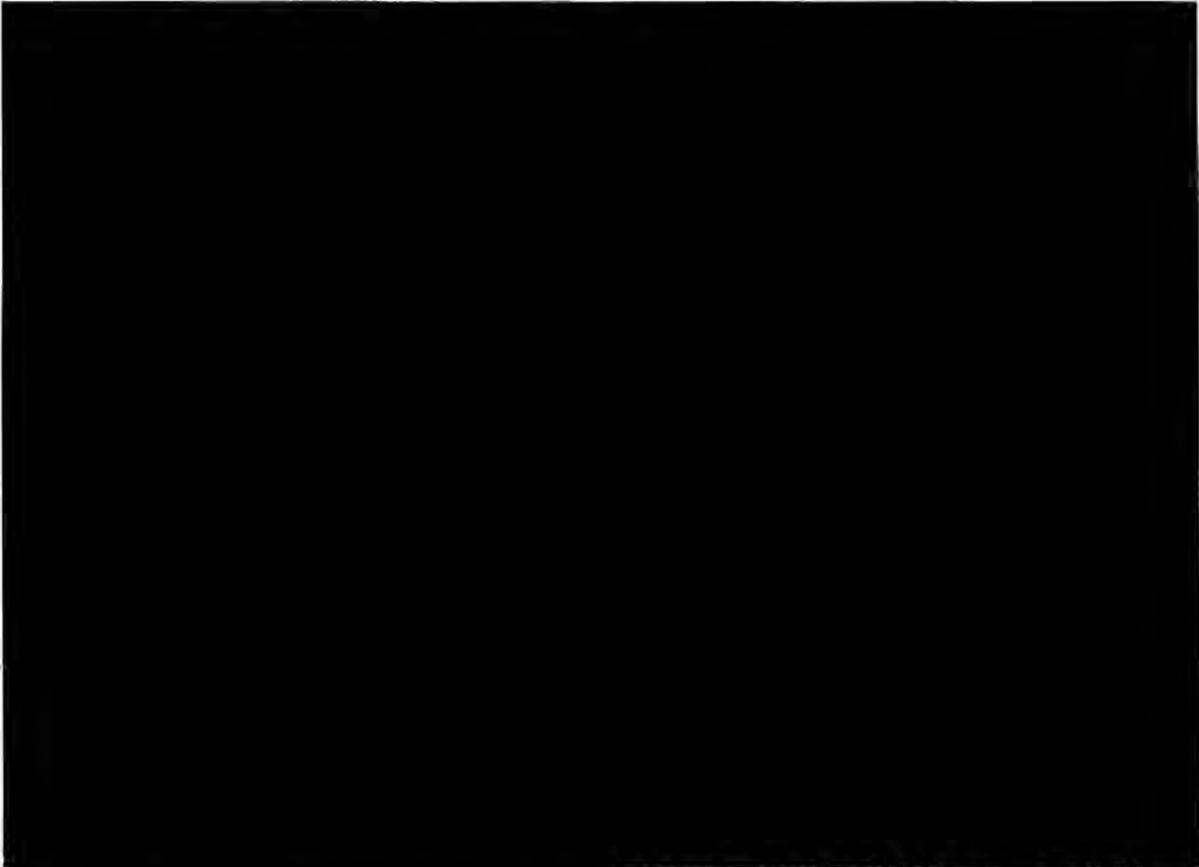
¹⁶ Section 104 of FISA speaks only of the Attorney General, but section 101(g) defines "Attorney General" to include the Deputy Attorney General. *See* 50 U.S.C. § 1801(g). (TS//SI-STLW//NF)

¹⁷ *See also* 50 U.S.C. § 1810 (providing for civil liability as well). (TS//SI-STLW//NF)

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

purposes. Indeed, this exclusivity is expressly emphasized in section 2511(2)(f), which states that "procedures in this chapter or chapter 121 [addressing access to stored wire and electronic communications and customer records] and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted." *Id.* § 2511(2)(f) (2000 & Supp. I 2001). (~~FS//SI- STELLAR WIND~~)



As we explain in Part II.B, a proper analysis of STELLAR WIND must not consider FISA in isolation. Rather, it must take into account the Congressional Authorization for Use of Military Force. We conclude that the Congressional Authorization is critical for STELLAR WIND in two respects. First, its plain terms can properly be understood as an express authorization for surveillance targeted specifically at al Qaeda and affiliated terrorist organizations. The Congressional Authorization effectively exempts such surveillance from the requirements of FISA. Second, even if it does not provide such express



~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

~~TOP SECRET//COMINT STELLAR WIND//NOFORN~~

authority, at a minimum the Congressional Authorization creates sufficient ambiguity concerning the application of FISA that it justifies applying the canon of constitutional avoidance to construe the Congressional Authorization and FISA in conjunction such that FISA does not preclude the surveillance ordered by the President in STELLAR WIND. Finally, in Part II.C we explain that, even if constitutional narrowing could not be applied to avoid a conflict between STELLAR WIND and FISA, the content collection the President has ordered, which specifically targets communications of the enemy in time of war, would be lawful because the restrictions of FISA would be unconstitutional as applied in this context as an impermissible infringement on the President's constitutional powers as Commander in Chief. ~~(TS//SI-STLW//NF)~~

A. Prior Opinions of this Office – Constitutional Avoidance (U)

Reading FISA to prohibit the content collection the President has ordered in STELLAR WIND would, at a minimum, raise serious doubts about the constitutionality of the statute. As we explain in greater detail below, *see* Part II.C.1, the President has inherent constitutional authority to conduct warrantless electronic surveillance for foreign intelligence purposes. Indeed, it was established at the time FISA was enacted that the President had such an inherent constitutional power. *See, e.g., United States v. Butenko*, 494 F.2d 593 (3d Cir. 1974) (*en banc*). A statute that purports to eliminate the President's ability to exercise what the courts have recognized as an inherent constitutional authority – particularly a statute that would eliminate his ability to conduct that surveillance during a time of armed conflict for the express purpose of thwarting attacks on the United States – at a minimum raises serious constitutional questions. ~~(TS//SI-STLW//NF)~~

When faced with a statute that may present an unconstitutional infringement on the powers of the President, our first task is to determine whether the statute may be construed to avoid the constitutional difficulty. As the Supreme Court has explained, “if an otherwise acceptable construction of a statute would raise serious constitutional problems, and where an alternative interpretation of the statute is ‘fairly possible,’ we are obligated to construe the statute to avoid such problems.” *INS v. St. Cyr*, 533 U.S. 289, 299-300 (2001) (citations omitted); *see also Crowell v. Benson*, 285 U.S. 22, 62 (1932) (“When the validity of an act of the Congress is drawn in question, and even if a serious doubt of constitutionality is raised, it is a cardinal principle that this Court will first ascertain whether a construction of the statute is fairly possible by which the question may be avoided.”); *Ashwander v. TVA*, 297 U.S. 288, 345-48 (1936) (Brandeis, J., concurring). In part, this rule of construction reflects a recognition that Congress should be presumed to act constitutionally and that one should not “lightly assume that Congress intended to . . . usurp power constitutionally forbidden it.” *Edward J. DeBartolo Corp. v. Florida Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575 (1988). As a result, “when a particular interpretation of a statute invokes the outer limits of Congress’ power, we expect a clear indication that Congress intended that result.” *St. Cyr*, 533 U.S. at 299; *see also NLRB v. Catholic Bishop of Chicago*, 440 U.S. 490, 506-07 (1979). (U)

This Office has always adhered to the rule of construction described above and generally will apply all reasonable interpretive tools to avoid an unconstitutional encroachment upon the

~~TOP SECRET//COMINT STELLAR WIND//NOFORN~~

~~TOP SECRET~~ [REDACTED] /COMINT-~~STELLAR WIND~~ [REDACTED] /NOFORN

President's constitutional powers where such an interpretation is possible. *Cf. Franklin v. Massachusetts*, 505 U.S. 788, 800-01 (1992) ("Out of respect for the separation of powers and the unique constitutional position of the President, we find that textual silence is not enough to subject the President to the provisions of the [Administrative Procedure Act]. We would require an express statement by Congress before assuming it intended the President's performance of his statutory duties to be reviewed for abuse of discretion."). As the Supreme Court has recognized, moreover, the canon of constitutional avoidance has particular importance in the realm of national security and national defense, where the President's constitutional authority is at its highest. *See Department of the Navy v. Egan*, 484 U.S. 518, 527, 530 (1988) (explaining that presidential authority to protect classified information flows directly from a "constitutional investment of power in the President" and that as a result "unless Congress specifically has provided otherwise, courts traditionally have been reluctant to intrude upon the authority of the Executive in military and national security affairs"); William N. Eskridge, Jr., *Dynamic Statutory Interpretation* 325 (1994) (describing "[s]uper-strong rule against congressional interference with the president's authority over foreign affairs and national security"); *cf. Public Citizen v. Department of Justice*, 491 U.S. 440, 466 (1989) ("Our reluctance to decide constitutional issues is especially great where, as here, they concern the relative powers of coordinate branches of government."). Thus, this Office will typically construe a general statute, even one that is written in unqualified terms, to be implicitly limited so as not to infringe on the President's Commander-in-Chief powers. *Cf. id.* at 464-66 (applying avoidance canon even where statute created no ambiguity on its face). Only if Congress provides a clear indication that it is attempting to regulate the President's authority as Commander in Chief and in the realm of national security will we construe the statute to apply.¹⁹ (U)

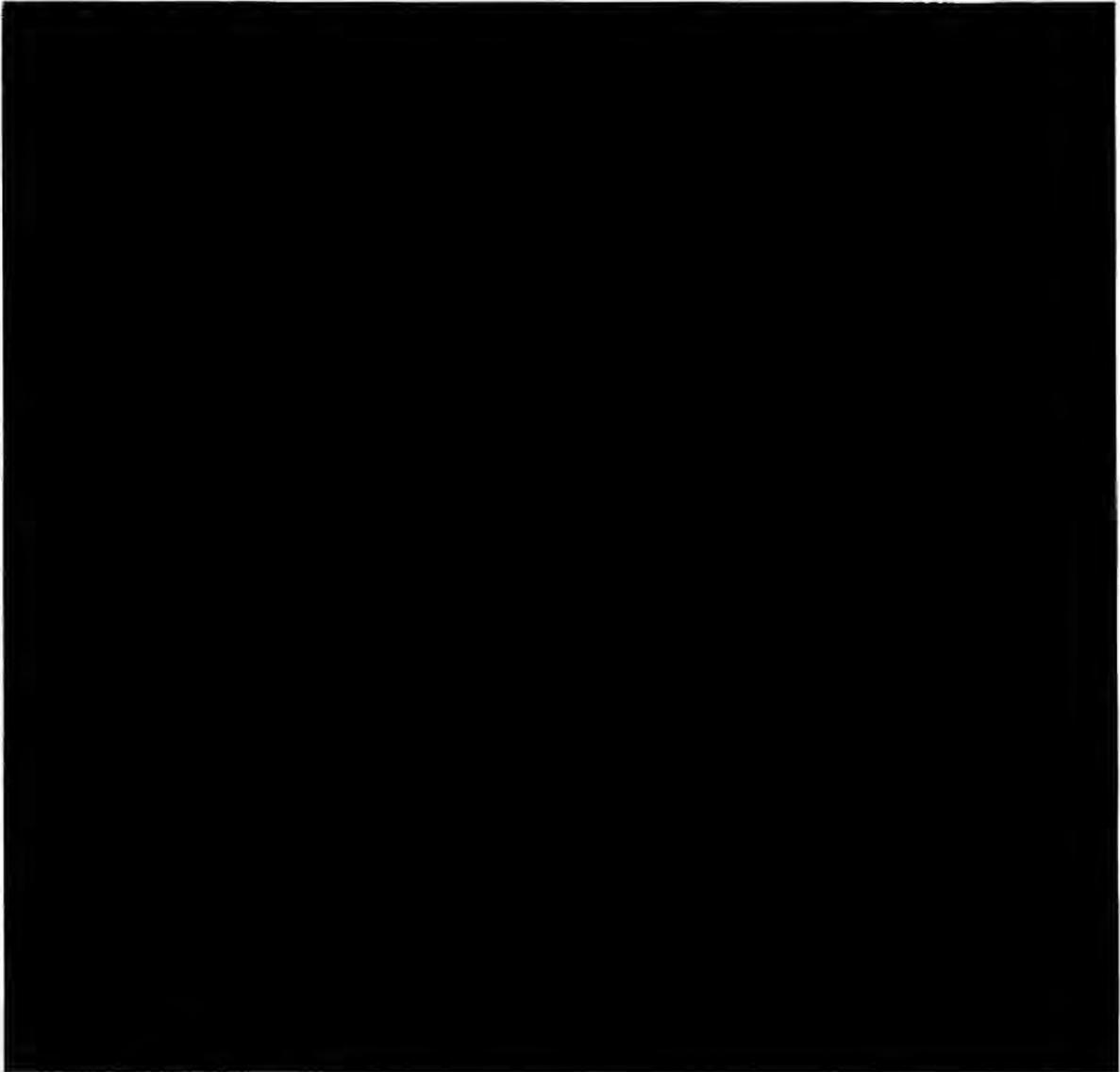
The constitutional avoidance canon, however, can be used to avoid a serious constitutional infirmity in a statute only if a construction avoiding the problem is "fairly possible," *Crowell v. Benson*, 285 U.S. at 62, and not in cases where "Congress specifically has provided otherwise," *Egan*, 484 U.S. at 530. "Statutes should be construed to avoid constitutional questions, but this interpretive canon is not a license . . . to rewrite language

¹⁹ For example, this Office has concluded that, despite statutory restrictions upon the use of Title III wiretap information and restrictions on the use of grand jury information under Federal Rule of Criminal Procedure 6(e), the President has an inherent constitutional authority to receive all foreign intelligence information in the hands of the government necessary for him to fulfill his constitutional responsibilities and that statutes and rules should be understood to include an implied exception so as not to interfere with that authority. *See* Memorandum for the Deputy Attorney General from Jay S. Bybee, Assistant Attorney General, Office of Legal Counsel, *Re: Effect of the Patriot Act on Disclosure to the President and Other Federal Officials of Grand Jury and Title III Information Relating to National Security and Foreign Affairs* 1 (July 22, 2002); Memorandum for Frances Fragos Townsend, Counsel, Office of Intelligence Policy and Review, from Randolph D. Moss, Assistant Attorney General, Office of Legal Counsel, *Re: Title III Electronic Surveillance Material and the Intelligence Community* 13-14 (Oct. 17, 2000); Memorandum for Gerald A. Schroeder, Acting Counsel, Office of Intelligence Policy and Review, from Richard L. Shiffrin, Deputy Assistant Attorney General, Office of Legal Counsel, *Re: Grand Jury Material and the Intelligence Community* 14-17 (Aug. 14, 1997); *see also Rainbow Navigation, Inc. v. Department of the Navy*, 783 F.2d 1072, 1078 (D.C. Cir. 1986) (Scalia, J.) (suggesting that an "essentially domestic statute" might have to be understood as "subject to an implied exception in deference to" the President's "constitutionally conferred powers as commander-in-chief" that the statute was not meant to displace). (U)

~~TOP SECRET~~ [REDACTED] /COMINT-~~STELLAR WIND~~ [REDACTED] /NOFORN

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

enacted by the legislature." *Salinas v. United States*, 522 U.S. 52, 59-60 (1997) (internal quotation marks omitted). If Congress has made it clear that it intends FISA to provide a comprehensive restraint on the Executive's ability to conduct foreign intelligence surveillance, then the question whether FISA's constraints are unconstitutional cannot be avoided
(TS//SI-STLW//NF)



~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

Pages 25 – 28

Withheld in Full

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

B. Analysis of STELLAR WIND Under FISA Must Take Into Account the September 2001 Congressional Authorization for Use of Military Force ~~(TS//SI-STLW//NF)~~

In the particular context of STELLAR WIND, however, FISA cannot properly be examined in isolation. Rather, analysis must also take into account the Congressional Authorization for Use of Military Force passed specifically in response to the September 11 attacks. As explained below, that Congressional Authorization is properly read to provide explicit authority for the targeted content collection undertaken in STELLAR WIND. Moreover, even if it did not itself provide authority for STELLAR WIND, at a minimum the Congressional Authorization makes the application of FISA in this context sufficiently ambiguous that the canon of constitutional avoidance properly applies to avoid a conflict here between FISA and STELLAR WIND. ~~(TS//SI-STLW//NF)~~

1. The Congressional Authorization provides express authority for STELLAR WIND content collection ~~(TS//SI-STLW//NF)~~

On September 18, 2001 Congress voted to authorize the President "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001." Congressional Authorization § 2(a). In authorizing "all necessary and appropriate force" (emphasis added), the Authorization necessarily included the use of signals intelligence capabilities, which are a critical, and traditional, tool for finding the enemy so that destructive force can be brought to bear on him. The Authorization, moreover, expressly gave the President authority to undertake activities both domestically and overseas. Thus, the operative terms state that the President is authorized to use force "in order to prevent any future acts of international terrorism against the United States," *id.*, an objective which, given the recent attacks within the Nation's borders and the continuing use of combat air patrols throughout the country at the time Congress acted, certainly contemplated the possibility of military action within the United States. The preambulatory clauses, moreover, recite that the United States should exercise its rights "to protect United States citizens both *at home* and abroad." *Id.* *publ.* (emphasis added). As commentators have acknowledged, the broad terms of the Congressional Authorization "creat[e] very nearly plenary presidential power to conduct the present war on terrorism, through the use of military and other means, against enemies both abroad and possibly even within the borders of the United States, as identified by the President, and without apparent limitation as to duration, scope, and tactics." Michael Stokes Paulsen, *Youngstown Goes to War*, 19 Const. Comment. 215, 222-23 (2002); *see also id.* at 252 (stating that the Authorization "constitutes a truly extraordinary congressional grant to the President of extraordinary discretion in the use of military power for an indefinite period of time"). (U)

The application of signals intelligence activities to international communications to detect communications between enemy forces and persons within the United States should be understood to fall within the Congressional Authorization because intercepting such communications has been a standard practice of Commanders in Chief in past major conflicts

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

~~TOP SECRET//COMINT-**██████████**STELLAR WIND-**██████████**//NOFORN~~

where there was any possibility of an attack on the United States. As early as the Civil War, the "advantages of intercepting military telegraphic communications were not long overlooked. [Confederate] General Jeb Stuart actually had his own personal wiretapper travel along with him in the field." Samuel Dash et al., *The Eavesdroppers* 23 (1971). Shortly after Congress declared war on Germany in World War I, President Wilson (citing only his constitutional powers and the declaration of war) ordered the censorship of messages sent outside the United States via submarine cables, telegraph and telephone lines. See Exec. Order No. 2604 (Apr. 28, 1917) (attached at Tab G).²³ A few months later, the Trading with the Enemy Act authorized government censorship of "communications by mail, cable, radio, or other means of transmission passing between the United States and any foreign country." Pub. L. No. 65-91, § 3(d), 40 Stat. 411, 413 (1917). On December 8, 1941, the day after Pearl Harbor was attacked, President Roosevelt gave the Director of the FBI "temporary powers to direct all news censorship and to control all other telecommunications traffic in and out of the United States." Jack A. Gottschalk, "Consistent with Security" . . . *A History of American Military Press Censorship*, 5 Comm. & L. 35, 39 (1983) (emphasis added); see also Memorandum for the Secretary of War, Navy, State, Treasury, Postmaster General, Federal Communications Commission, from Franklin D. Roosevelt (Dec. 8, 1941), in *Official and Confidential File of FBI Director J. Edgar Hoover*, Microfilm Reel 3, Folder 60 (attached at Tab I). President Roosevelt soon supplanted that temporary regime by establishing an Office of Censorship in accordance with the War Powers Act of 1941. See Pub. L. No. 77-354, § 303, 55 Stat. 838, 840-41 (Dec. 18, 1941); Gottschalk, 5 Comm. & L. at 40. The censorship regime gave the government access to "communications by mail, cable, radio, or other means of transmission passing between the United States and any foreign country." *Id.*; see also Exec. Order No. 8985, § 1, 6 Fed. Reg. 6625, 6625 (Dec. 19, 1941) (attached at Tab J). In addition, the United States government systematically listened surreptitiously to electronic communications as part of the war effort. See Dash, *Eavesdroppers* at 30 ("During [World War II] wiretapping was used extensively by military intelligence and secret service personnel in combat areas abroad, as well as by the FBI and secret service in this country."). (~~TS//SI-STLW/NF~~)

In light of such prior wartime practice, the content collection activities conducted under STELLAR WIND appear to fit squarely within the sweeping terms of the Congressional Authorization. The use of signals intelligence to identify and pinpoint the enemy is a traditional component of wartime military operations employed to defeat the enemy and to prevent enemy attacks in the United States. Here, as in other conflicts, it happens that the enemy may use public communications networks, and some of the enemy may already be in the United States. While those factors may be present in this conflict to a greater degree than in the past, neither is novel. Moreover, both factors were well known at the time Congress acted. Wartime interception of international communications on public networks to identify communications that may be of assistance to the enemy should thus be understood as one of the standard methods of dealing

²³ The scope of the order was later extended to encompass messages sent to "points without the United States or to points on or near the Mexican border through which messages may be despatched for purpose of evading the censorship herein provided." Exec. Order No. 2967 (Sept. 26, 1918) (attached at Tab H). (~~TS//SI-STLW/NF~~)

~~TOP SECRET//COMINT-**██████████**STELLAR WIND-**██████████**//NOFORN~~

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

with the enemy that Congress can be presumed to have authorized in giving its approval to "all necessary and appropriate force" that the President would deem required to defend the Nation. Congressional Authorization § 2(a) (emphasis added).²⁴ (TS//SI-STLW//NF)

Content collection under STELLAR WIND, moreover, is specifically targeted at communications for which there is a reason to believe that one of the communicants is an agent of al Qaeda or one of its affiliated organizations. The content collection is thus, as the terms of the Congressional Authorization indicate, directed "against those . . . organizations, or persons [the President] determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001" and is undertaken "in order to prevent any future acts of international terrorism against the United States."²⁵ Congressional Authorization § 2(a). As noted above, section 111 of FISA, 50 U.S.C. § 1811, provides that the President may undertake electronic surveillance without regard to the restrictions in FISA for a period of 15 days after a congressional declaration of war. The legislative history of FISA indicates that this exception was limited to 15 days because that period was thought sufficient for the President to secure legislation easing the restrictions of FISA for the conflict at hand. See H.R. Conf. Rep. No. 95-1720, at 34, reprinted in 1978 U.S.C.C.A.N. 4048, 4063 (stating that "the conferees intend that this period will allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency"). The Congressional Authorization functions as precisely such legislation: it is emergency legislation passed to address a specific armed conflict and expressly designed to authorize whatever military actions the Executive deems appropriate to safeguard the United States. In it the Executive sought and received a blanket authorization from Congress for all uses of the military against al Qaeda that might be necessary to prevent future terrorist attacks against the United States. The mere fact that the Authorization does not expressly amend FISA is not material. By its plain terms it gives clear authorization for "all necessary and appropriate force" against al Qaeda that the President deems required "to protect United States citizens both at home and abroad" from those (including al Qaeda) who "planned, authorized, committed, or aided" the September 11 attacks. Congressional Authorization pmb.,

²⁴ In other contexts, we have taken a similar approach to interpreting the Congressional Authorization. Thus, for example, detaining enemy combatants is also a standard part of warfare. As a result, we have concluded that the Congressional Authorization expressly authorizes such detentions, even of American citizens. See Memorandum for Daniel J. Bryant, Assistant Attorney General, Office of Legislative Affairs, from John C. Yoo, Deputy Assistant Attorney General, Office of Legal Counsel, *Re: Applicability of 18 U.S.C. § 4001(a) to Military Detention of United States Citizens* 6 (June 27, 2002); accord *Hamdi v. Rumsfeld*, 316 F.3d 450, 467 (4th Cir. 2003) (holding that "capturing and detaining enemy combatants is an inherent part of warfare" and that the "'necessary and appropriate force' referenced in the congressional resolution necessarily includes" such action), cert. granted, 124 S. Ct. 981 (2004). But see *Padilla v. Rumsfeld*, 352 F.3d 695, 722-23 (2d Cir. 2003) (holding that, except "in the battlefield context where detentions are necessary to carry out the war," the Congressional Authorization is not sufficiently "clear" and "unmistakable" to override the restrictions on detaining U.S. citizens in § 4001), cert. granted, 124 S. Ct. 1353 (2004). (U)

²⁵ As noted above, see *supra* pp. 16, 17, STELLAR WIND content-collection authority is limited to communications suspected to be those of al Qaeda, al Qaeda-affiliated organizations and other international terrorist groups that the President determines both (i) are in armed conflict with the United States and (ii) pose a threat of hostile action within the United States. [REDACTED]

(TS//SI-STLW//NF)

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

~~TOP SECRET// [REDACTED] //COMINT- STELLAR WIND [REDACTED] //NOFORN~~

§ 2(a). It is perfectly natural that Congress did not attempt to single out into subcategories every aspect of the use of the armed forces it was authorizing, for as the Supreme Court has recognized, even in normal times outside the context of a crisis "Congress cannot anticipate and legislate with regard to every possible action the President may find it necessary to take." *Dames & Moore v. Regan*, 453 U.S. 654, 678 (1981). Moreover, when dealing with military affairs, Congress may delegate in broader terms than it uses in other areas. See, e.g., *Loving v. United States*, 517 U.S. 748, 772 (1996) (noting that "the same limitations on delegation do not apply" to duties that are linked to the Commander-in-Chief power); cf. *Zemel v. Rusk*, 381 U.S. 1, 17 (1965) ("[B]ecause of the changeable and explosive nature of contemporary international relations . . . Congress - in giving the Executive authority over matters of foreign affairs - must of necessity paint with a brush broader than that it customarily wields in domestic areas."). Thus, the Congressional Authorization can be treated as the type of wartime exception that was contemplated in FISA's legislative history. Even if FISA had not envisioned legislation limiting the application of FISA in specific conflicts, the Congressional Authorization, as a later-in-time - and arguably more specific - statute must prevail over FISA to the extent of any inconsistency.²⁶ (TS//SI-STLW//NF)

The Congressional Authorization contains another provision that is particularly significant in this context. Congress expressly recognized that "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States." Congressional Authorization, pmb1. That provision gives express congressional recognition to the President's inherent constitutional authority to take action to defend the United States even without congressional support. That is a striking recognition of presidential authority from Congress, for while the courts have long acknowledged an inherent authority in the President to take action to protect Americans abroad, see, e.g., *Durand v. Hollins*, 8 F. Cas. 111, 112 (C.C.S.D.N.Y. 1860) (No. 4186), and to protect the Nation from attack, see, e.g., *The Prize Cases*, 67 U.S. (2 Black) 635, 668 (1863), at least since the War Powers Resolution, Pub. L. No. 93-148, 87 Stat. 555 (1973), codified at 50 U.S.C. §§ 1541-1548, there has been no comparable recognition of such inherent authority by Congress, and certainly not a sweeping recognition of authority such as that here. Cf. 50 U.S.C. § 1541(c) (recognizing President's inherent constitutional authority to use force in response to an attack on the United States). This provision cannot be discounted, moreover, as mere exuberance in the immediate aftermath of September 11, for the same terms were repeated by Congress more than a year later in the Authorization for Use of Military Force Against Iraq Resolution of 2002. Pub. L. No. 107-243,

²⁶ It is true that repeals by implication are disfavored and we should attempt to construe two statutes as being "capable of co-existence." *Ruckelshaus v. Monsanto*, 467 U.S. 986, 1017, 1018 (1984). In this instance, however, the ordinary restrictions in FISA cannot continue to apply if the Congressional Authorization is appropriately construed to have its full effect. The ordinary constraints in FISA would preclude the President from doing precisely what the Congressional Authorization allows: using "all necessary and appropriate force . . . to prevent any future acts of international terrorism against the United States" by al Qaeda. Congressional Authorization § 2(a). Not only did the Congressional Authorization come later than FISA, but it is also more specific in the sense that it applies only to a particular conflict, whereas FISA is a general statute intended to govern all "electronic surveillance" (as defined in 50 U.S.C. § 1801(f)). If FISA and the Congressional Authorization "irreconcilabl[y] conflict," then the Congressional Authorization must prevail over FISA to the extent of the inconsistency. See *Radzanower v. Touche Ross & Co.*, 426 U.S. 148, 154 (1976). (TS//SI-STLW//NF)

~~TOP SECRET// [REDACTED] //COMINT- STELLAR WIND [REDACTED] //NOFORN~~

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

pmb1., 116 Stat. 1498, 1500 (Oct. 16, 2002) (“[T]he President has authority under the Constitution to take action in order to deter and prevent acts of international terrorism against the United States . . .”). That recognition of inherent authority, moreover, is particularly significant in the FISA context because, as explained above, one of the specific amendments implemented by FISA was removing any acknowledgment from section 2511(3) of title 18 of the Executive’s inherent constitutional authority to conduct foreign intelligence surveillance. At least in the context of the conflict with al Qaeda, however, Congress appears to have acknowledged a sweeping inherent Executive authority to “deter and prevent” attacks that logically should include the ability to carry out signals intelligence activities necessary to detect such planned attacks. (TS//SI-STLW//NF)

To be sure, the broad construction of the Congressional Authorization outlined above is not without some difficulties. Some countervailing considerations might be raised to suggest that the Authorization should not be read to extend into the field covered by FISA. In particular, shortly after the Authorization was passed Congress turned to consider a number of legislative proposals from the Administration, some of which specifically amended FISA. *See, e.g.*, USA PATRIOT Act, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291 (Oct. 26, 2001) (amending section 104(a)(7)(B) of FISA to require that the acquisition of foreign intelligence information be a “significant purpose” of the surveillance order being sought, rather than “the purpose”). Thus, it might be argued that the Congressional Authorization cannot properly be construed to grant the President authority to undertake electronic surveillance without regard to the restrictions in FISA because, if the Congressional Authorization actually had applied so broadly, the specific amendments to FISA that Congress passed a few weeks later in the PATRIOT Act would have been superfluous. (TS//SI-STLW//NF)

We do not think, however, that the amendments to FISA in the PATRIOT Act can justify narrowing the broad terms of the Congressional Authorization. To start with, the Authorization addresses the use of the armed forces solely in the context of the particular armed conflict of which the September 11 attacks were a part. To come within the scope of the Authorization, surveillance activity must be directed “against those nations, organizations, or persons [the President] determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001.” Congressional Authorization § 2(a). The Authorization thus eliminates the restrictions of FISA solely for that category of foreign intelligence surveillance cases. Subsequent amendments to FISA itself, however, modified the authorities for foreign intelligence surveillance in *all* cases, whether related to the particular armed conflict with al Qaeda or not. Given the broader impact of such amendments, it cannot be said that they were superfluous even if the Congressional Authorization broadly authorized electronic surveillance directed against al Qaeda and affiliated organizations. (TS//SI-STLW//NF)

That understanding is bolstered by an examination of the specific amendments to FISA that were passed, because each addressed a shortcoming in FISA that warranted a remedy for all efforts to gather foreign intelligence, not just for efforts in the context of an armed conflict, much less the present one against al Qaeda. Indeed, some addressed issues that had been identified as requiring a legislative remedy long before the September 11 attacks occurred. For these

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

~~TOP SECRET//COMINT STELLAR WIND//NOFORN~~

amendments, the September 11 attacks merely served as a catalyst for spurring legislative change that was required in any event. For example, Congress changed the standard required for the certification from the government to obtain a FISA order from a certification that "the purpose" of the surveillance was obtaining foreign intelligence to a certification that "a significant purpose" of the surveillance was obtaining foreign intelligence. See USA PATRIOT Act § 218, 115 Stat. at 291 (codified at 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B)). That change was designed to help dismantle the "wall" that had developed separating criminal investigations from foreign intelligence investigations within the Department of Justice. See generally *In re Sealed Case*, 310 F.3d 717, 725-30 (Foreign Intel. Surv. Ct. of Rev. 2002). The "wall" had been identified as a significant problem hampering the government's efficient use of foreign intelligence information well before the September 11 attacks and in contexts unrelated to terrorism. See, e.g., *Final Report of the Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation* 710, 729, 732 (May 2000); General Accounting Office, *FBI Intelligence Investigations: Coordination Within Justice on Counterintelligence Criminal Matters Is Limited* (GAO-01-780) 3, 31 (July 2001). Indeed, this Office was asked as long ago as 1995 to consider whether, under the terms of FISA as it then existed, an application for a surveillance order could be successful without establishing that the "primary" purpose of the surveillance was gathering foreign intelligence. See Memorandum for Michael Vatis, Deputy Director, Executive Office for National Security, from Walter Dellinger, Assistant Attorney General, Office of Legal Counsel, *Re: Standards for Searches Under Foreign Intelligence Surveillance Act* (Feb. 14, 1995). The PATRIOT Act thus provided the opportunity for addressing a longstanding shortcoming in FISA that had an impact on foreign intelligence gathering generally. (U)

Similarly, shortly after the PATRIOT Act was passed, the Administration sought additional legislation expanding to 72 hours (from 24 hours) the time period the government has for filing an application with the FISC after the Attorney General has authorized the emergency initiation of electronic surveillance. See Intelligence Authorization Act for Fiscal Year 2002, Pub. L. No. 107-108, § 314(a), 115 Stat. 1394, 1402 (Dec. 28, 2001). That change was also needed for the proper functioning of FISA generally, not simply for surveillance of agents of al Qaeda. In the wake of the September 11 attacks, there was bound to be a substantial increase in the volume of surveillance conducted under FISA, which would strain existing resources. As a result, it was undoubtedly recognized that, in order for the emergency authority to be useful as a practical matter in any foreign intelligence case, the Department of Justice would need more than 24 hours to prepare applications after initiating emergency surveillance. Similar broadly based considerations underpinned the other amendments to FISA that were enacted in the fall of 2001. (TS//SI-STLW//NF)

As a result, we conclude that the enactment of amendments to FISA after the passage of the Congressional Authorization does not compel a narrower reading of the broad terms of the Authorization. The unqualified terms of the Congressional Authorization are broad enough on their face to include authority to conduct signals intelligence activity within the United States. We believe that the Congressional Authorization can thus be read to provide specific authority during this armed conflict that overrides the limitations in FISA. The Supreme Court has

~~TOP SECRET//COMINT STELLAR WIND//NOFORN~~

~~TOP SECRET//COMINT//STELLAR WIND//NOFORN~~

repeatedly made clear that in the field of foreign affairs and particularly in the field of war powers and national security, congressional enactments will be broadly construed where they indicate support for the exercise of Executive authority. *See, e.g., Haig v. Agee*, 453 U.S. 280, 293-303 (1981); *United States ex rel. Knauff v. Shaughnessy*, 338 U.S. 537, 543-45 (1950); *cf. Agee*, 453 U.S. at 291 (in "the areas of foreign policy and national security . . . congressional silence is not to be equated with congressional disapproval"); *Dames & Moore v. Regan*, 453 U.S. 654, 678-82 (1981) (even where there is no express congressional authorization, legislation in related field may be construed to indicate congressional acquiescence in Executive action). Here, the broad terms of the Congressional Authorization are easily read to encompass authority for signals intelligence activities directed against al Qaeda and its affiliates. ~~(TS//SI//STLW//NF)~~

2. At a minimum, the Congressional Authorization bolsters the case for applying the canon of constitutional avoidance ~~(TS//SI//STLW//NF)~~

Even if we did not believe that the Congressional Authorization provided a clear result on this point, at the very least the Congressional Authorization – which was expressly designed to give the President broad authority to respond to the threat posed by al Qaeda as he saw fit – creates a significant ambiguity concerning whether the restrictions of FISA apply to electronic surveillance undertaken in the context of the conflict with al Qaeda. That ambiguity decisively tips the scales in favor of applying the canon of constitutional avoidance to construe the Congressional Authorization and FISA in combination so that the restrictions of FISA do not apply to the President's actions as Commander in Chief in attempting to thwart further terrorist attacks on the United States. As noted above, in this wartime context the application of FISA to restrict the President's ability to conduct surveillance he deems necessary to detect and disrupt further attacks would raise grave constitutional questions. The additional ambiguity created by the Congressional Authorization suffices, in our view, to warrant invoking the canon of constitutional avoidance and thus justifies reading the Congressional Authorization to eliminate the constitutional issues that would otherwise arise if FISA were construed to limit the Commander in Chief's ability to conduct signals intelligence to thwart terrorist attacks. Application of the canon is particularly warranted, moreover, given Congress's express recognition in the terms of its Authorization that the President has inherent authority under the Constitution to take steps to protect the Nation against attack. The final preambulatory clause of the Authorization squarely states that "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States." Congressional Authorization pmbl. As commentators have recognized, this clause "constitutes an extraordinarily sweeping congressional recognition of independent presidential *constitutional* power to employ the war power to combat terrorism." Paulsen, 19 Const. Comment. at 252. That congressional recognition of inherent presidential authority bolsters the conclusion that, when FISA and the Congressional Authorization are read together, the canon of constitutional avoidance should be applied because it cannot be said that Congress has unequivocally indicated an intention to risk a constitutionally dubious exercise of power by restricting the authority of the Commander in Chief to conduct signals intelligence in responding to the terrorist attacks. ~~(TS//SI//STLW//NF)~~

~~TOP SECRET//COMINT//STELLAR WIND//NOFORN~~

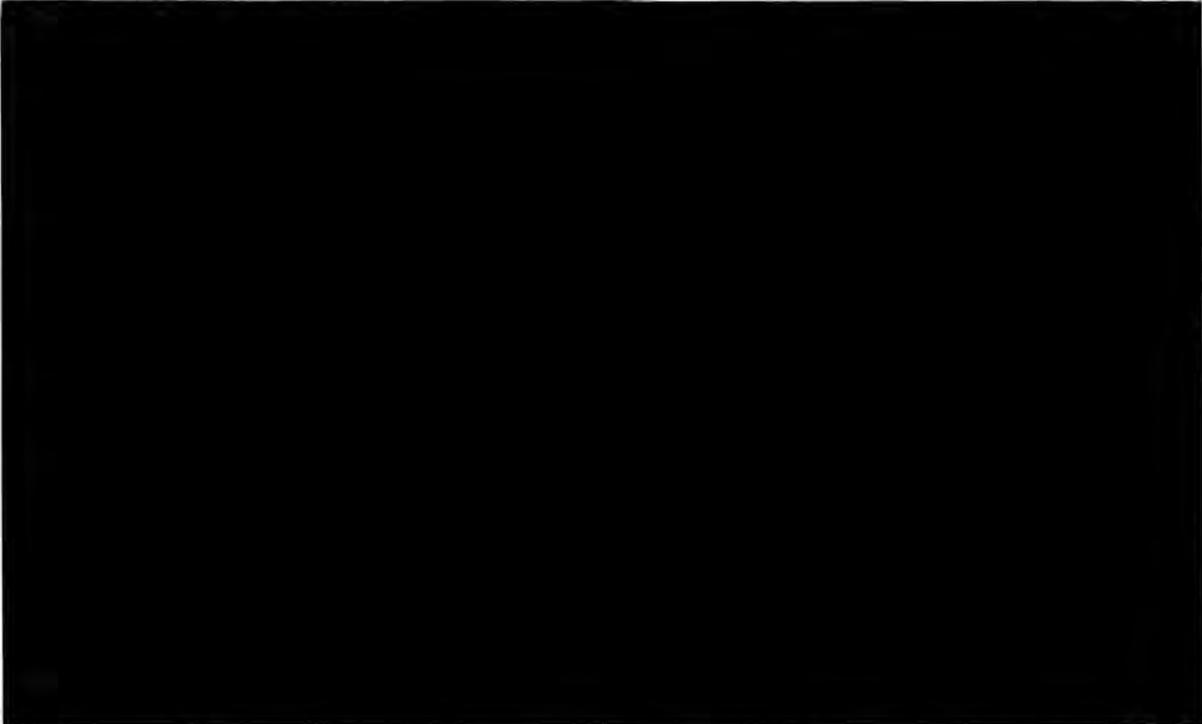
~~TOP SECRET// [REDACTED] /COMINT- STELLAR WIND [REDACTED] /NOFORN~~

In sum, the constitutional avoidance canon is properly applied to conclude that the Congressional Authorization removes the restrictions of FISA for electronic surveillance undertaken by the Department of Defense and directed "against those nations, organizations, or persons [the President] determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001."²⁷ [REDACTED]

[REDACTED] fits that description.²⁸ (TS//SI-STLW//NF)



As a result, we believe that a thorough and prudent approach to analyzing the legality of STELLAR WIND must also take into account the possibility that FISA may be read as prohibiting the electronic surveillance activities at issue here. We turn to that analysis below. (TS//SI-STLW//NF)



~~TOP SECRET// [REDACTED] /COMINT- STELLAR WIND [REDACTED] /NOFORN~~

~~TOP SECRET//COMINT//STELLAR WIND//NOFORN~~

C. If FISA Purported To Prohibit Targeted, Wartime Surveillance Against the Enemy Under STELLAR WIND, It Would Be Unconstitutional as Applied (TS//SI//STLW//NF)

Assuming that FISA cannot be interpreted to avoid the constitutional issues that arise if it does, in fact, [REDACTED] we must next examine whether FISA, as applied in the particular circumstances of surveillance directed by the Commander in Chief in the midst of an armed conflict and designed to detect and prevent attacks upon the United States, is unconstitutional. We conclude that it is. (TS//SI//STLW//NF)

I. Even in peacetime, absent congressional action, the President has inherent constitutional authority, consistent with the Fourth Amendment, to order warrantless foreign intelligence surveillance (TS//SI//STLW//NF)

We begin our analysis by setting to one side for the moment both the particular wartime context at issue here and the statutory constraints imposed by FISA to examine the pre-existing constitutional authority of the President in this field in the absence of any action by Congress. It has long been established that, even in peacetime, the President has an inherent constitutional authority, consistent with the Fourth Amendment, to conduct warrantless searches for foreign intelligence purposes. The Constitution vests power in the President as Commander in Chief of the armed forces, *see* U.S. Const. art. II, § 2, and, in making him Chief Executive, grants him authority over the conduct of the Nation's foreign affairs. As the Supreme Court has explained, "[t]he President is the sole organ of the nation in its external relations, and its sole representative with foreign nations." *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 319 (1936) (internal quotation marks and citations omitted). These sources of authority grant the President inherent power both to take measures to protect national security information, *see, e.g., Department of the Navy v. Egan*, 484 U.S. 518, 527 (1988), and more generally to protect the security of the Nation from foreign attack. *Cf. The Prize Cases*, 67 U.S. (2 Black) 635, 668 (1863). To carry out these responsibilities, the President must have authority to gather information necessary for the execution of his office. The Founders, after all, intended the President to be clothed with all authority necessary to carry out the responsibilities assigned to him as Commander in Chief and Chief Executive. *See, e.g., The Federalist* No. 23, at 147 (Alexander Hamilton) (Jacob E. Cooke ed. 1961) (explaining that the federal government will be "cloathed with all the powers requisite to the complete execution of its trust"); *id.* No. 41, at 269 (James Madison) ("Security against foreign danger is one of the primitive objects of civil society. . . . The powers requisite for attaining it must be effectually confided to the federal councils."); *see also Johnson v. Eisentrager*, 339 U.S. 763, 788 (1950) ("The first of the enumerated powers of the President is that he shall be Commander-in-Chief of the Army and Navy of the United States. And, of course, grant of war power includes all that is necessary and proper for carrying these powers into execution." (citation omitted)). Thus, it has long been recognized that he has authority to hire spies, *see, e.g., Totten v. United States*, 92 U.S. 105, 106 (1876), and his authority to collect intelligence necessary for the conduct of foreign affairs has frequently been acknowledged. *See Chicago & S. Air Lines v. Waterman S.S. Corp.*, 333 U.S.

~~TOP SECRET//COMINT//STELLAR WIND//NOFORN~~

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

103, 111 (1948) ("The President, both as Commander-in-Chief and as the Nation's organ for foreign affairs, has available intelligence services whose reports neither are nor ought to be published to the world."); *Curtiss-Wright*, 299 U.S. at 320 ("He has his confidential sources of information. He has his agents in the form of diplomatic, consular and other officials.")
(TS//SI-STLW//NF)

When it comes to collecting foreign intelligence information within the United States, of course, the President must exercise his inherent authorities consistently with the requirements of the Fourth Amendment.²⁹ Determining the scope of the President's inherent constitutional authority in this field, therefore, requires analysis of the requirements of the Fourth Amendment – at least to the extent of determining whether or not the Fourth Amendment imposes a warrant requirement on searches conducted for foreign intelligence purposes. If it does, then a statute such as FISA that also imposes a procedure for judicial authorization cannot be said to encroach upon authorities the President would otherwise have.³⁰ (TS//SI-STLW//NF)

The Fourth Amendment prohibits "unreasonable searches and seizures" and directs that "no Warrants shall issue, but upon probable cause." U.S. Const. amend. IV. In "the criminal context," as the Supreme Court has pointed out, "reasonableness usually requires a showing of probable cause" and a warrant. *Board of Educ. v. Earls*, 536 U.S. 822, 828 (2002). The warrant and probable cause requirement, however, is far from universal. Rather, the "Fourth Amendment's central requirement is one of reasonableness," and the rules the Court has developed to implement that requirement "[s]ometimes . . . require warrants." *Illinois v. McArthur*, 531 U.S. 326, 330 (2001); see also, e.g., *Earls*, 536 U.S. at 828 ("The probable cause standard, however, is peculiarly related to criminal investigations and may be unsuited to determining the reasonableness of administrative searches where the Government seeks to prevent the development of hazardous conditions." (emphasis added; internal quotation marks omitted)). (U)

In particular, the Supreme Court has repeatedly made clear that in situations involving "special needs" that go beyond a routine interest in law enforcement, there may be exceptions to the warrant requirement. Thus, the Court has explained that there are circumstances "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995) (quoting *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987)); see also *McArthur*, 531 U.S. at 330 ("We nonetheless have made it clear that there are exceptions to the warrant requirement. When faced with special law enforcement needs, diminished expectations of privacy, minimal

²⁹ The Fourth Amendment does not protect aliens outside the United States. See *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990). (U)

³⁰ We assume for purposes of the discussion here that content collection under STELLAR WIND is subject to the requirements of the Fourth Amendment. In Part V of this memorandum, we address the reasonableness under the Fourth Amendment of the specific kinds of collection that occur under STELLAR WIND. In addition, we note that there may be a basis for concluding that STELLAR WIND is a military operation to which the Fourth Amendment does not even apply. See *infra* n.84. (TS//SI-STLW//NF)

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

TOP SECRET//COMINT//STELLAR WIND//NOFORN

intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable.”). It is difficult to encapsulate in a nutshell the different circumstances the Court has found qualifying as “special needs” justifying warrantless searches. But generally when the government faces an increased need to be able to react swiftly and flexibly, or when there are interests in public safety at stake beyond the interests in law enforcement, the Court has found the warrant requirement inapplicable. (U)

Thus, among other things, the Court has permitted warrantless searches to search property of students in public schools, see *New Jersey v. T.L.O.*, 469 U.S. 325, 340 (1985) (noting that warrant requirement would “unduly interfere with the maintenance of the swift and informal disciplinary procedures needed in the schools”), to screen athletes and students involved in extra-curricular activities at public schools for drug use, see *Vernonia*, 515 U.S. at 654-655; *Earls*, 536 U.S. at 829-38, and to conduct drug testing of railroad personnel involved in train accidents, see *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 634 (1989). Indeed, in many special needs cases the Court has even approved suspicionless searches or seizures. See, e.g., *Earls*, 536 U.S. at 829-38 (suspicionless drug testing of public school students involved in extra-curricular activities); *Michigan Dep't of State Police v. Sitz*, 496 U.S. 444, 449-55 (1990) (road block to check all motorists for signs of drunken driving); *United States v. Martinez-Fuerte*, 428 U.S. 543, 562 (1976) (road block near the border to check vehicles for illegal immigrants). But see *City of Indianapolis v. Edmond*, 531 U.S. 32, 41 (2000) (striking down use of roadblock to check for narcotics activity because its “primary purpose was to detect evidence of ordinary criminal wrongdoing”). (U)

The field of foreign intelligence collection presents another case of “special needs beyond the normal need for law enforcement” where the Fourth Amendment’s touchstone of reasonableness can be satisfied without resort to a warrant. In foreign intelligence investigations, the targets of surveillance are agents of foreign powers who may be specially trained in concealing their activities from our government and whose activities may be particularly difficult to detect. The Executive requires a greater degree of flexibility in this field to respond with speed and absolute secrecy to the ever-changing array of foreign threats it faces. The object of searches in this field, moreover, is securing information necessary to protect the national security from the hostile designs of foreign powers, including even the possibility of a foreign attack on the Nation. (TS//SI//STLW//NF)

Given those distinct interests at stake, it is not surprising that every federal court that has ruled on the question has concluded that, even in peacetime, the President has inherent constitutional authority, consistent with the Fourth Amendment, to conduct searches for foreign intelligence purposes without securing a judicial warrant. See *United States v. Clay*, 430 F.2d 165, 172 (5th Cir. 1970); *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973); *United States v. Butenko*, 494 F.2d 593 (3d Cir. 1974) (en banc); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977); *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980). But cf. *Zweibon v. Mitchell*, 516 F.2d 594 (D.C. Cir. 1975) (en banc) (dictum in plurality opinion suggesting that warrant would be required even in foreign intelligence investigation). (TS//SI//STLW//NF)

TOP SECRET//COMINT//STELLAR WIND//NOFORN

~~TOP SECRET//COMINT--STELLAR WIND-//NOFORN~~

To be sure, the Supreme Court has left this precise question open. In *United States v. United States District Court*, 407 U.S. 297 (1972) (*Keith*), the Supreme Court concluded that the Fourth Amendment's warrant requirement applies to investigations of purely domestic threats to security – such as domestic terrorism. The Court made clear, however, that it was not addressing Executive authority to conduct foreign intelligence surveillance: “[T]he instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country.” *Id.* at 308; see also *id.* at 321-322 & n.20 (“We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents.”). (TS//SI-STLW//NF)

Indeed, four of the courts of appeals noted above decided – after *Keith*, and expressly taking *Keith* into account – that the President has inherent authority to conduct warrantless surveillance in the foreign intelligence context. As the Fourth Circuit observed in *Truong*, “the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would . . . unduly frustrate the President in carrying out his foreign affairs responsibilities.” 629 F.2d at 913 (internal quotation marks omitted). The court pointed out that a warrant requirement would be a hurdle that would reduce the Executive's flexibility in responding to foreign threats that “require the utmost stealth, speed, and secrecy.” *Id.* It also would potentially jeopardize security by increasing “the chance of leaks regarding sensitive executive operations.” *Id.* It is true that the Supreme Court had discounted such concerns in the domestic security context, see *Keith*, 407 U.S. at 319-20, but as the Fourth Circuit explained, in dealing with hostile agents of foreign powers, the concerns are arguably more compelling. More important, in the area of foreign intelligence the expertise of the Executive is paramount. While courts may be well-adapted to ascertaining whether there is probable cause to believe that a crime under domestic law has been committed, they would be ill-equipped to review executive determinations concerning the need to conduct a particular search or surveillance to secure vital foreign intelligence. See *Truong*, 629 F.2d at 913-14. Cf. *Curtiss-Wright*, 299 U.S. at 320 (“[The President] has the better opportunity of knowing the conditions which prevail in foreign countries, and especially is this true in time of war. He has his confidential sources of information.”). It is not only the Executive's expertise that is critical, moreover. As the Fourth Circuit pointed out, the Executive has a constitutionally superior position in matters pertaining to foreign affairs and national security: “Perhaps most crucially, the executive branch not only has superior expertise in the area of foreign intelligence, it is also constitutionally designated as the pre-eminent authority in foreign affairs.” *Truong*, 629 F.2d at 914. The court thus concluded that there was an important separation of powers interest in not having the judiciary intrude on the field of foreign intelligence collection: “[T]he separation of powers requires us to acknowledge the principal responsibility of the President for foreign affairs and concomitantly for foreign intelligence surveillance.” *Id.*; cf. *Haig v. Agee*, 453 U.S. 280, 292 (1981) (“Matters intimately related to foreign policy and national security are rarely proper subjects for judicial intervention.”). We agree with that analysis.³¹ (TS//SI-STLW//NF)

³¹ In addition, there is a further basis on which *Keith* is readily distinguished. As *Keith* made clear, one of the significant concerns driving the Court's conclusion in the domestic security context was the inevitable connection between perceived threats to domestic security and political dissent. As the Court explained: “Fourth

~~TOP SECRET//COMINT--STELLAR WIND-//NOFORN~~

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

In the specific context of STELLAR WIND, moreover, the case for inherent executive authority to conduct surveillance in the absence of congressional action is substantially stronger for at least two reasons. First and foremost, all of the precedents outlined above addressed inherent executive authority under the foreign affairs power to conduct surveillance *in a routine peacetime context*.³² They did not even consider the authority of the Commander in Chief to gather intelligence in the context of an ongoing armed conflict in which the mainland United States had already been under attack and in which the intelligence-gathering efforts at issue were designed to thwart further armed attacks. The case for inherent executive authority is necessarily much stronger in the latter scenario, which is precisely the circumstance presented by STELLAR WIND. (TS//SI-STLW//NF)

Second, it also bears noting that in the 1970s the Supreme Court had barely started to develop the "special needs" jurisprudence of warrantless searches under the Fourth Amendment. The first case usually considered part of that line of decisions is *United States v. Martinez-Fuerte*, 428 U.S. 543, decided in 1976 – after three courts of appeals decisions addressing warrantless foreign intelligence surveillance had already been handed down. The next Supreme Court decision applying a rationale clearly in the line of "special needs" jurisprudence was not until 1985, see *New Jersey v. T.L.O.*, 469 U.S. 325,³³ and the jurisprudence was not really developed until the 1990s. Thus, the courts of appeals decisions described above all decided in favor of an inherent executive authority to conduct warrantless foreign intelligence searches even before the Supreme Court had clarified the major doctrinal developments in Fourth Amendment law that now provide the clearest support for such an authority. (TS//SI-STLW//NF)

Executive practice, of course, also demonstrates a consistent understanding that the President has inherent constitutional authority, in accordance with the dictates of the Fourth Amendment, to conduct warrantless searches and surveillance within the United States for

Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.'" *Keith*, 407 U.S. at 314; see also *id.* at 320 ("Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent."). Surveillance of domestic groups necessarily raises a First Amendment concern that generally is not present when the subjects of the surveillance are the agents of foreign powers.

One of the important factors driving the Supreme Court's conclusion that the warrant requirement should apply in the domestic security context is thus simply absent in the foreign intelligence realm. (TS//SI-STLW//NF)

³² The surveillance in *Truong*, while in some sense connected to the Vietnam conflict and its aftermath, took place in 1977 and 1978, see 629 F.2d at 912, after the close of active hostilities. (TS//SI-STLW//NF)

³³ The term "special needs" appears to have been coined by Justice Blackmun in his concurrence in *T.L.O.* See 469 U.S. at 351 (Blackmun, J., concurring in judgment). (TS//SI-STLW//NF)

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

~~TOP SECRET// [REDACTED] #COMINT- STELLAR WIND [REDACTED] //NOFORN~~

foreign intelligence purposes. Wiretaps for such purposes have been authorized by Presidents at least since the administration of Roosevelt in 1940. *See, e.g., United States v. United States District Court*, 444 F.2d 651, 669-71 (6th Cir. 1971) (reproducing as an appendix memoranda from Presidents Roosevelt, Truman, and Johnson). Before the passage of FISA in 1978, all foreign intelligence wiretaps and searches were conducted without any judicial order pursuant to the President's inherent authority. *See, e.g., Truong*, 629 F.2d at 912-14; *United States v. Bin Laden*, 126 F. Supp. 2d 264, 273 (S.D.N.Y. 2000) ("Warrantless foreign intelligence collection has been an established practice of the Executive Branch for decades."). When FISA was first passed, moreover, it addressed solely electronic surveillance and made no provision for physical searches. *See* Pub. L. No. 103-359, § 807, 108 Stat. 3423, 3443-53 (1994) (adding provision for physical searches). As a result, after a brief interlude during which applications for orders for physical searches were made to the FISC despite the absence of any statutory procedure, the Executive continued to conduct searches under its own inherent authority. Indeed, in 1981, the Reagan Administration, after filing an application with the FISC for an order authorizing a physical search, filed a memorandum with the court explaining that the court had no jurisdiction to issue the requested order and explaining that the search could properly be conducted without a warrant pursuant to the President's inherent constitutional authority. *See* S. Rep. No. 97-280, at 14 (1981) ("The Department of Justice has long held the view that the President and, by delegation, the Attorney General have constitutional authority to approve warrantless physical searches directed against foreign powers or their agents for intelligence purposes."). This Office has also repeatedly recognized the constitutional authority of the President to engage in warrantless surveillance and searches for foreign intelligence purposes.³⁴ (~~TS//SI- STELLAR WIND~~)



Intelligence – Warrantless Electronic Surveillance – Common Carriers, 2 Op. O.L.C. 123 (1978); *Warrantless Foreign Intelligence Surveillance – Use of Television – Beepers*, 2 Op. O.L.C. 14, 15 (1978) ("[T]he President can authorize warrantless electronic surveillance of an agent of a foreign power, pursuant to his constitutional power to gather foreign

~~TOP SECRET// [REDACTED] #COMINT- STELLAR WIND [REDACTED] //NOFORN~~

~~TOP SECRET//COMINT--STELLAR WIND-/NOFORN~~

These examples, too, all relate to assertions of executive authority in a routine, peacetime context. Again, the President's authority is necessarily heightened when he acts during wartime as Commander-in-Chief to protect the Nation from attack. Thus, not surprisingly, as noted above, Presidents Wilson and Roosevelt did not hesitate to assert executive authority to conduct surveillance – through censoring communications – upon the outbreak of war. *See supra* p. 30. (TS//SI-STLW//NF)

2. FISA is unconstitutional as applied in this context (TS//SI-STLW//NF)

While it is thus uncontroversial that the President has inherent authority to conduct warrantless searches for foreign intelligence purposes in the absence of congressional action, the restrictions imposed in FISA present a distinct question: whether the President's constitutional authority in this field is exclusive, or whether Congress may, through FISA, impose a requirement to secure judicial authorization for such searches. To be more precise, analysis of STELLAR WIND presents an even narrower question: namely, whether, in the context of an ongoing armed conflict, Congress may, through FISA, impose restrictions on the means by which the Commander in Chief may use the capabilities of the Department of Defense to gather intelligence about the enemy in order to thwart further foreign attacks on the United States. (TS//SI-STLW//NF)

As discussed below, the conflict of congressional and executive authority in this context presents a difficult question – one for which there are few if any precedents directly on point in the history of the Republic. In almost every previous instance in which the country has been threatened by war or imminent foreign attack and the President has taken extraordinary measures to secure the national defense, Congress has acted to support the Executive through affirmative legislation granting the President broad wartime powers,⁵⁵ or else the Executive has acted in

intelligence." (TS//SI-STLW//NF)

⁵⁵ As explained above, we believe that the better construction of the Congressional Authorization for Use of Military Force in the present conflict is that it also reflects precisely such a congressional endorsement of Executive action and authorizes the content collection undertaken in STELLAR WIND. In this part of our analysis, however, we are assuming, in the alternative, that the Authorization cannot be read so broadly and that FISA by its

~~TOP SECRET//COMINT--STELLAR WIND-/NOFORN~~

TOP SECRET//~~COMINT~~ STELLAR WIND//NOFORN

exigent circumstances in the absence of any congressional action whatsoever (for example, President Lincoln's actions in 1861 in proclaiming a blockade of the southern States and instituting conscription). In the classic separation of powers analysis set out by Justice Jackson in *Youngstown*, such circumstances describe either "category I" situations – where the legislature has provided an "express or implied authorization" for the Executive – or "category II" situations – where Congress may have some shared authority over the subject, but has chosen not to exercise it. See *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635-37 (1952); see also *Dames & Moore v. Regan*, 453 U.S. 654, 668-69 (1981) (generally following Jackson's framework). Here, however, we confront an exercise of Executive authority that falls into "category III" of Justice Jackson's classification. See 343 U.S. at 637-38. The President (for purposes of this argument in the alternative) is seeking to exercise his authority as Commander in Chief to conduct intelligence surveillance that Congress has expressly restricted by statute. (TS//SI-STLW//NF)

At bottom, therefore, analysis of the constitutionality of FISA in the context of STELLAR WIND centers on two questions: (i) whether the signals intelligence collection the President wishes to undertake is such a core exercise of Commander-in-Chief control over the armed forces during armed conflict that Congress cannot interfere with it at all or, (ii) alternatively, whether the particular restrictions imposed by FISA are such that their application would impermissibly frustrate the President's exercise of his constitutionally assigned duties as Commander in Chief. (TS//SI-STLW//NF)

As a background for that context-specific analysis, however, we think it is useful first to examine briefly the constitutional basis for Congress's assertion of authority in FISA to regulate the President's inherent powers over foreign intelligence gathering even in the general, peacetime context. Even in that non-wartime context, the assertion of authority in FISA, and in particular the requirement that the Executive seek orders for surveillance from Article III courts, is not free from constitutional doubt. Of course, if the constitutionality of some aspects of FISA is open to any doubt even in the run-of-the-mill peacetime context, it follows *a fortiori* that the legitimacy of congressional encroachments on Executive power will only be more difficult to sustain where they involve trenching upon decisions of the Commander in Chief in the midst of a war. Thus, after identifying some of the questions surrounding the congressional assertion of authority in FISA generally, we proceed to the specific analysis of FISA as applied in the wartime context of STELLAR WIND. (TS//SI-STLW//NF)

- a. Even outside the context of wartime surveillance of the enemy, the scope of Congress's power to restrict the President's inherent authority to conduct foreign intelligence surveillance is unclear. (TS//SI-STLW//NF)

To frame the analysis of the specific, wartime operation of STELLAR WIND, it is important to note at the outset that, even in the context of general foreign intelligence collection

terms prohibits the STELLAR WIND content collection absent an order from the FISC. (TS//SI-STLW//NF)

TOP SECRET//~~COMINT~~ STELLAR WIND//NOFORN

~~TOP SECRET//COMINT--STELLAR WIND-//NOFORN~~

in non-wartime situations, the source and scope of congressional power to restrict executive action through FISA is somewhat uncertain. We start from the fundamental proposition that in assigning to the President as Chief Executive the preeminent role in handling the foreign affairs of the Nation, the Constitution grants substantive powers to the President. As explained above, the President's role as sole organ for the Nation has long been recognized as carrying with it substantive powers in the field of national security and foreign intelligence. This Office has traced the source of this authority to the Vesting Clause of Article II, which states that "[t]he executive Power shall be vested in a President of the United States of America." U.S. Const. art. II, § 1. Thus, we have explained that the Vesting Clause "has long been held to confer on the President plenary authority to represent the United States and to pursue its interests outside the borders of the country, subject only to limits specifically set forth in the Constitution itself and to such statutory limitations as the Constitution permits Congress to impose by exercising one of its enumerated powers" *The President's Compliance with the "Timely Notification" Requirement of Section 501(b) of the National Security Act*, 10 Op. O.L.C. 159, 160-61 (1986) ("*Timely Notification Requirement Op.*"). Significantly, we have concluded that the "conduct of secret negotiations and intelligence operations lies at the very heart of the President's executive power." *Id.* at 165. The President's authority in this field is sufficiently comprehensive that the entire structure of federal restrictions for protecting national security information has been created solely by presidential order, not by statute. *See generally Department of the Navy v. Egan*, 484 U.S. 518, 527, 530 (1988); *see also New York Times Co. v. United States*, 403 U.S. 713, 729-30 (1971) (Stewart, J., concurring) ("[I]t is the constitutional duty of the Executive – as a matter of sovereign prerogative and not as a matter of law as the courts know law – through the promulgation and enforcement of executive regulations, to protect the confidentiality necessary to carry out its responsibilities in the field of international relations and national defense."). Similarly, the NSA is entirely a creature of the Executive – it has no organic statute defining or limiting its functions. (TS//SI-//NF)

Moreover, it is settled beyond dispute that, although Congress is also granted some powers in the area of foreign affairs, certain presidential authorities in that realm are wholly beyond the power of Congress to interfere with by legislation. For example, as the Supreme Court explained in *Curtiss-Wright*, the President "makes treaties with the advice and consent of the Senate; but he alone negotiates. Into the field of negotiations the Senate cannot intrude; and Congress itself is powerless to invade it." 299 U.S. at 319. Similarly, President Washington established early in the history of the Republic the Executive's absolute authority to maintain the secrecy of negotiations with foreign powers, even against congressional efforts to secure information. *Id.* at 320-21 (quoting Washington's 1796 message to the House of Representatives regarding documents relative to the Jay Treaty). Recognizing presidential authority in this field, this Office has stated that "congressional legislation authorizing extraterritorial diplomatic and intelligence activities is superfluous, and . . . statutes infringing the President's inherent Article II authority would be unconstitutional." *Timely Notification Requirement Op.*, 10 Op. O.L.C. at 164. (U)

Whether the President's power to conduct foreign intelligence searches within the United States is one of the inherent presidential powers with which Congress cannot interfere presents a

~~TOP SECRET//COMINT--STELLAR WIND-//NOFORN~~

TOP SECRET//COMINT//STELLAR WIND//NOFORN

difficult question. It is not immediately obvious which of Congress's enumerated powers in the field of foreign affairs would provide authority to regulate the President's use of constitutional methods of collecting foreign intelligence. Congress has authority to "regulate Commerce with foreign Nations," to impose "Duties, Imposts and Excises," and to "define and punish Piracies and Felonies committed on the high Seas, and Offenses against the Law of Nations" U.S. Const. art. I, § 8, cls. 1, 3, 10. But none of those powers suggests a specific authority to regulate the Executive's intelligence-gathering activities. Of course, the power to regulate both foreign and interstate commerce gives Congress authority generally to regulate the facilities that are used for carrying communications, and that may arguably provide Congress sufficient authority to limit the interceptions the Executive can undertake. A general power to regulate commerce, however, provides a weak basis for interfering with the President's preeminent position in the field of national security and foreign intelligence. Intelligence gathering, after all, is as this Office has stated before, at the "heart" of Executive functions. Since the time of the Founding it has been recognized that matters requiring secrecy – and intelligence in particular – are quintessentially Executive functions. *See, e.g., The Federalist No. 64, at 435 (John Jay)* ("The convention have done well therefore in so disposing of the power of making treaties, that although the president must in forming them act by the advice and consent of the senate, yet he will be able to manage the business of intelligence in such manner as prudence may suggest.")³⁶ (TS//SI//STLW//NF)

³⁶ Two other congressional powers – the power to "make Rules for the Government and Regulation of the land and naval Forces," and the Necessary and Proper Clause, U.S. Const. art. I, § 8, cls. 14, 18 – are even less likely sources for congressional authority in this context. (TS//SI//STLW//NF)

As this Office has previously noted, the former clause should be construed as authorizing Congress to "prescrib[e] a code of conduct governing military life" rather than to "control actual military operations." Letter from Hon. Arlen Specter, U.S. Senate, from Charles J. Cooper, Assistant Attorney General, Office of Legal Counsel 8 (Dec. 16, 1987); *see also Chappell v. Wallace*, 462 U.S. 296, 301 (1983) (noting that the clause responded to the need to establish "rights, duties, and responsibilities in the framework of the military establishment, including regulations, procedures, and remedies related to military discipline"); *cf.* Memorandum for William J. Haynes, II, General Counsel, Department of Defense, from Jay S. Bybee, Assistant Attorney General, Office of Legal Counsel, *Re: The President's Power as Commander in Chief to Transfer Captured Terrorists to the Control and Custody of Foreign Nations* 6 (Mar. 13, 2002) (Congress's authority to make rules for the government and regulation of the land and naval forces is limited to the discipline of U.S. troops, and does not extend to "the rules of engagement and treatment concerning enemy combatants"). (U)

The Necessary and Proper Clause, by its own terms, allows Congress only to "carry[] into Execution" other powers granted in the Constitution. Such a power could not, of course, be used to limit or impinge upon one of those other powers (the President's inherent authority to conduct warrantless surveillance under the Commander-in-Chief power). *Cf. George K. Walker, United States National Security Law and United Nations Peacekeeping or Peacemaking Operations*, 29 Wake Forest L. Rev. 435, 479 (1994) ("The [Necessary and Proper] clause authorizes Congress to act with respect to its own functions as well as those of other branches except where the Constitution forbids it, or in the limited number of instances where exclusive power is specifically vested elsewhere. The power to preserve, protect, and defend, as Commander-in-Chief, is solely vested in the President. Thus, although the Congress might provide armed forces, Congress cannot dictate to the President how to use them.") (internal quotation marks and footnotes omitted); Saikrishna Prakash, *The Essential Meaning of Executive Power*, 2003 U. Ill. L. Rev. 701, 740 ("The Necessary and Proper Clause permits Congress to assist the president in the exercise of his powers; it does not grant Congress a license to reallocate or abridge powers already vested by the Constitution."). (U)

TOP SECRET//COMINT//STELLAR WIND//NOFORN

TOP SECRET//COMINT-~~STELLAR WIND~~//NOFORN

The legislative history of FISA amply demonstrates that the constitutional basis for the legislation was open to considerable doubt even at the time the statute was enacted and that even supporters of the bill recognized that the attempt to regulate the President's authority in this field presented an untested question of constitutional law that the Supreme Court might resolve by finding the statute unconstitutional. For example, while not opposing the legislation, Attorney General Levi nonetheless, when pressed by the Senate Judiciary Committee, testified that the President has an inherent constitutional power in this field "which cannot be limited, no matter what the Congress says." See *Foreign Intelligence Surveillance Act of 1976: Hearing Before the Subcomm. on Crim. Laws and Procs. of the Senate Comm. on the Judiciary*, 94th Cong. 17 (1976) ("1976 FISA Hearing"). Similarly, former Deputy Attorney General Laurence Silberman noted that previous drafts of the legislation had properly recognized that if the President had an inherent power in this field – "inherent," as he put it, "meaning beyond congressional control" – there should be a reservation in the bill acknowledging that constitutional authority. He concluded that the case for such a reservation was "probably constitutionally compelling." *Foreign Intelligence Electronic Surveillance: Hearings Before the Subcomm. on Legislation of the House Perm. Select Comm. on Intelligence* 217, 223 (1978) (statement of Laurence H. Silberman).³⁷ Senator McClellan, a member of the Judiciary Committee, noted his view that, as of 1974, given a constitutional power in the President to conduct warrantless intelligence surveillance, "no statute could change or alter it." *1976 FISA Hearing* at 2. And even if the law had developed since 1974, he still concluded in 1976 that "under any reasonable reading of the relevant court decisions, this bill approaches the outside limits of our Constitutional power to prescribe restrictions on and judicial participation in the President's responsibility to protect this country from threats from abroad, whether it be by electronic surveillance or other lawful means." *Id.* Indeed, the Conference Report took the unusual step of expressly acknowledging that, while Congress was attempting to foreclose the President's reliance on inherent constitutional authority to conduct surveillance outside the dictates of FISA, "the establishment by this act of exclusive means by which the President may conduct electronic surveillance does not foreclose a different decision by the Supreme Court." H.R. Conf. Rep. No. 95-1720, at 35, reprinted in 1978 U.S.C.C.A.N. 4048, 4064. The Conference Report thus effectively acknowledged that the congressional foray into regulating the Executive's inherent authority to conduct foreign intelligence surveillance – even in a non-war context – was sufficiently open to doubt that the statute might be struck down. (TS//SI-STLW//NF)

Even Senator Kennedy, one of the most ardent supporters of the legislation, acknowledged that it raised substantial constitutional questions that would likely have to be resolved by the Supreme Court. He admitted that "[i]f the President does have the [inherent constitutional] power [to engage in electronic surveillance for national security purposes], then depreciation of it in Congressional enactments cannot unilaterally diminish it. As with claims of

³⁷ The 2002 *per curiam* opinion of the Foreign Intelligence Surveillance Court of Review (for a panel that included Judge Silberman) noted that, in light of intervening Supreme Court cases, there is no longer "much left to an argument" that Silberman had made in his 1978 testimony about FISA's being inconsistent with "Article III case or controversy responsibilities of federal judges because of the secret, non-adversary process." *In re Sealed Case*, 310 F.3d 717, 732 n.19. That constitutional objection was, of course, completely separate from the one based upon the President's inherent powers. (TS//SI-STLW//NF)

TOP SECRET//COMINT-~~STELLAR WIND~~//NOFORN

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

Executive privilege and other inherent Presidential powers, the Supreme Court remains the final arbiter." 1976 FISA Hearing at 3. Moreover, Senator Kennedy and other senators effectively highlighted their own perception that the legislation might well go beyond the constitutional powers of Congress as they repeatedly sought assurances from Executive branch officials concerning the fact that "this President has indicated that he would be bound by [the legislation]" and speculated about "[h]ow binding is it going to really be in terms of future Presidents?" *Id.* at 16; see also *id.* at 23 (Sen. Hruska) ("How binding would that kind of a law be upon a successor President who would say . . . I am going to engage in that kind of surveillance because it is a power derived directly from the Constitution and cannot be inhibited by congressional enactment?"). The senators' emphasis on the current President's acquiescence in the legislation, and trepidation concerning the positions future Presidents might take, makes sense only if they were sufficiently doubtful of the constitutional basis for FISA that they conceived of the bill as more of a practical compromise between a particular President and Congress rather than an exercise of authority granted to Congress under the Constitution, which would necessarily bind future Presidents as the law of the land. (TS//SI-STLW//NF)

Finally, other members of Congress focused on the point that, whatever the scope of Congress's authority to impose some form of restriction on the President's conduct of foreign intelligence surveillance, the particular restriction imposed in FISA – requiring resort to an Article III court for a surveillance order – raised its own separation-of-powers problem. Four members of the House's Permanent Select Committee on Intelligence criticized this procedure on constitutional grounds and argued that it "would thrust the judicial branch into the arena of foreign affairs and thereby improperly subject 'political' decisions to 'judicial intrusion.'" H.R. Rep. No. 95-1283, Pt. 1, at 111 (1978). They concluded that it "is clearly inappropriate to inject the Judiciary into this realm of foreign affairs and national defense which is constitutionally delegated to the President and to the Congress." *Id.* at 114. Similar concerns about constitutionality were raised by dissenters from the Conference Report, who noted that "this legislation attempts to do that which it cannot do: transfer a constitutionally granted power from one branch of government to another." 124 Cong. Rec. 33,787, 33,788 (Oct. 5, 1978). (TS//SI-STLW//NF)

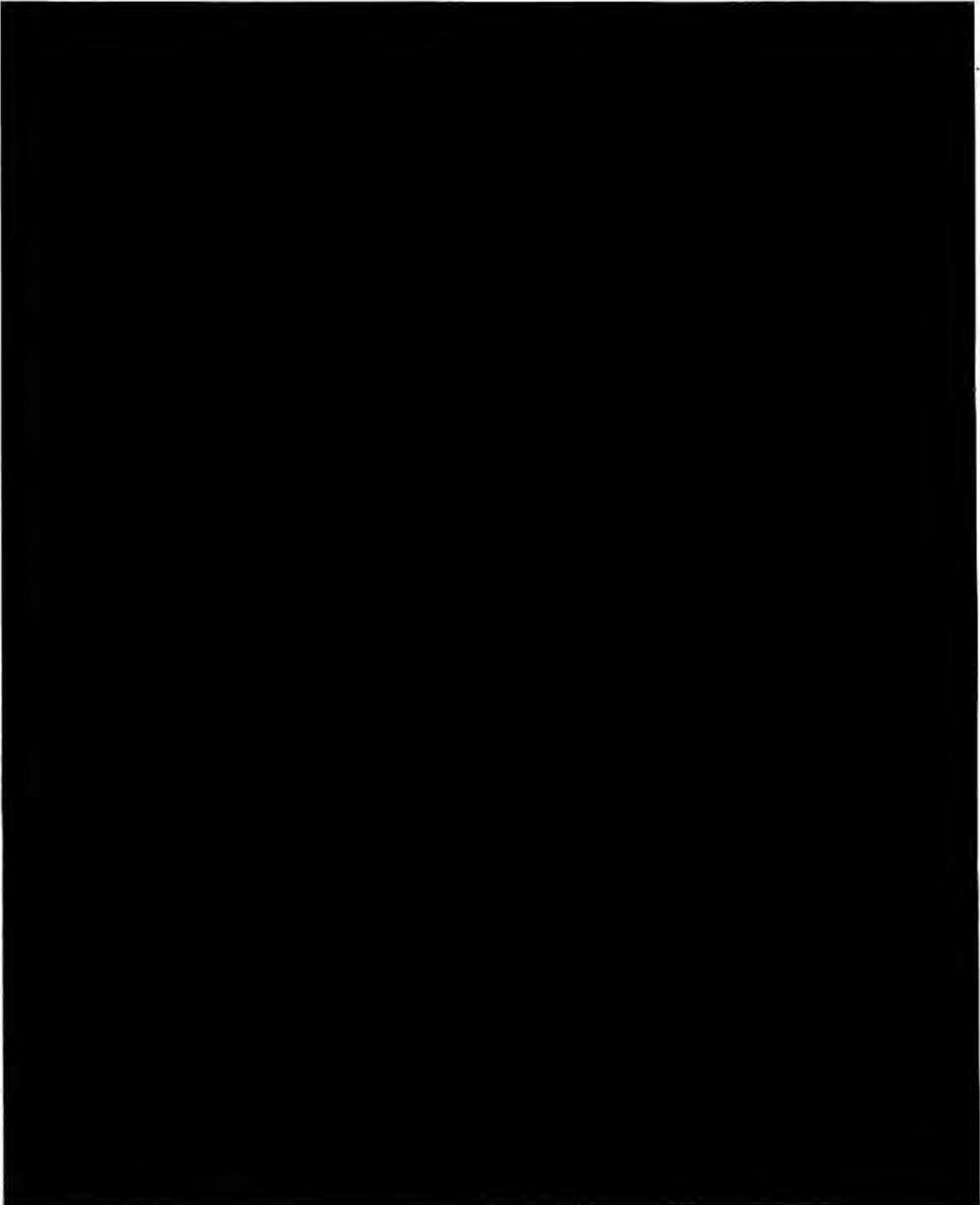
The only court that has addressed the relative powers of Congress and the President in this field, as far as we are aware, has suggested that the balance tips decidedly in the President's favor. The Foreign Intelligence Surveillance Court of Review recently noted that all courts to have addressed the issue have "held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information." *In re Sealed Case*, 310 F.3d 717, 742 (Foreign Intel. Surv. Ct. of Rev. 2002). On the basis of that unbroken line of precedent, the Court "[took] for granted that the President does have that authority," and concluded that, "assuming that is so, FISA could not encroach on the President's constitutional power." *Id.*³⁸ Although that statement was made without extended analysis, it is the only judicial statement on

³⁸ In the past, other courts have declined to express a view on that issue one way or the other. See, e.g., *Butenko*, 494 F.2d at 601 ("We do not intimate, at this time, any view whatsoever as the proper resolution of the possible clash of the constitutional powers of the President and Congress."). (TS//SI-STLW//NF)

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

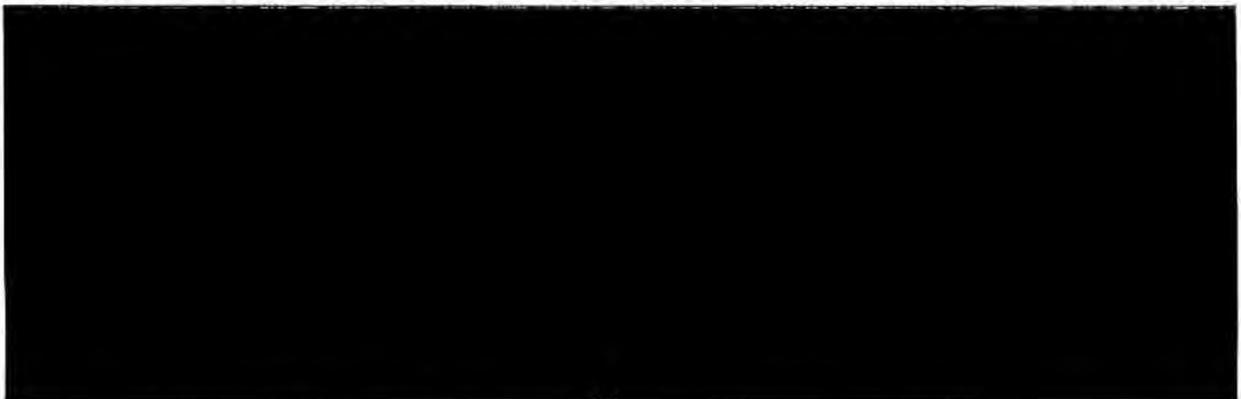
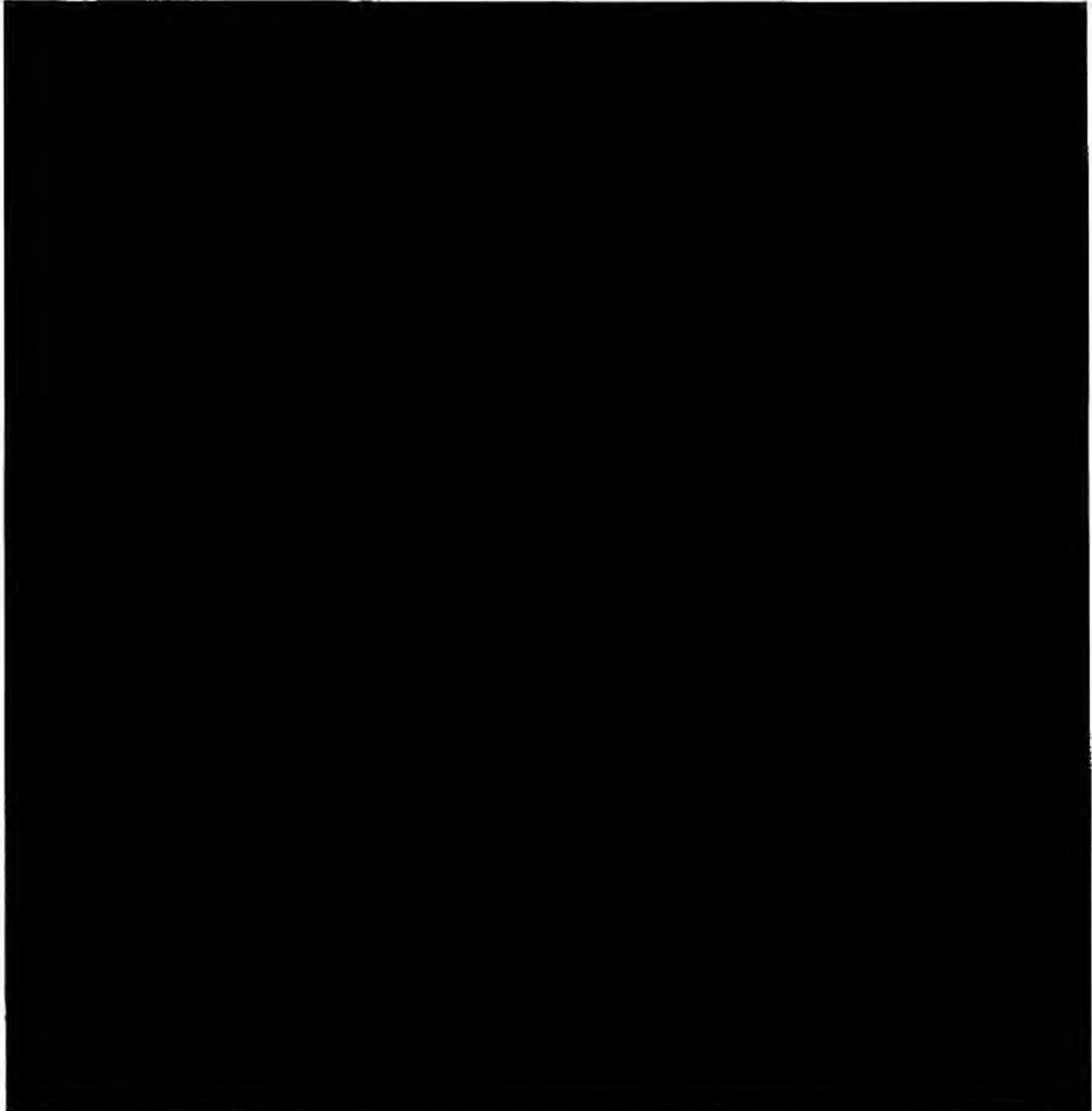
~~TOP SECRET// [REDACTED]//COMINT- STELLAR WIND [REDACTED]//NOFORN~~

point, and it comes from the specialized appellate court created expressly to deal with foreign intelligence issues under FISA. (TS//SI-STLW//NF)



~~TOP SECRET// [REDACTED]//COMINT- STELLAR WIND [REDACTED]//NOFORN~~

~~TOP SECRET~~ [REDACTED] /COMINT- STELLAR WIND [REDACTED] /NOFORN



~~TOP SECRET~~ [REDACTED] /COMINT- STELLAR WIND [REDACTED] /NOFORN

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

- b. In the narrow context of interception of enemy communications in the midst of an armed conflict, FISA is unconstitutional as applied (~~TS//SI-STLW//NF~~)

For analysis of STELLAR WIND, however, we need not address such a broad question, nor need we focus our analysis solely on the President's general authority in the realm of foreign affairs as Chief Executive. To the contrary, the activities authorized in STELLAR WIND are also – and indeed, primarily – an exercise of the President's authority as Commander in Chief. That authority, moreover, is being exercised in a particular factual context that involves using the resources of the Department of Defense in an armed conflict to defend the Nation from renewed attack at the hands of an enemy that has already inflicted the single deadliest foreign attack in the Nation's history. As explained above, each Presidential Authorization for a renewal of the STELLAR WIND authority is based on a review of current threat information from which the President concludes that al Qaeda

~~_____~~ March 11, 2004 Authorization ~~_____~~ In addition, the Authorization makes clear that the electronic surveillance is being authorized "for the purpose of detection and prevention of terrorist acts within the United States." *Id.* ~~_____~~ Surveillance designed to detect communications that may reveal critical information about an attack planned by enemy forces is a classic form of signals intelligence operation that is a key part of the military strategy for defending the country. Especially given that the enemy in this conflict has already demonstrated an ability to insert agents into the country surreptitiously to carry out attacks, the imperative demand for such intelligence as part of the military plan for defending the country is obvious. ~~_____~~

~~_____~~ Accordingly, our analysis focuses solely on those circumstances. It bears emphasis, moreover, that the question of congressional authority to regulate the Executive's powers to gather foreign intelligence has never been addressed in such a context. (~~TS//SI-STLW//NF~~)

Even in that narrow context, the conflict between the restrictions imposed by Congress in FISA and the President's inherent authorities as Commander in Chief presents a complex and in many respects novel question. As set out below, we now conclude that, at least in the narrow circumstances presented by STELLAR WIND in the current conflict with al Qaeda and its affiliated terrorist organizations, the President has exclusive constitutional authority, derived from his dual roles as Commander in Chief and sole organ for the Nation in foreign affairs, to

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

~~TOP SECRET//COMINT-**[REDACTED]**STELLAR WIND-**[REDACTED]**/NOFORN~~

order warrantless foreign intelligence surveillance targeted at communications of the enemy that Congress cannot override by legislation. Provisions in FISA that, by their terms, would prohibit the warrantless content collection undertaken under STELLAR WIND are thus unconstitutional as applied in this context. (TS//SI-STELW//NF)

As noted above, there are few precedents to provide concrete guidance concerning exactly where the line should be drawn defining core Commander-in-Chief authorities with which Congress cannot interfere. This Office has long concluded, based on decisions of the Supreme Court, that the Commander-in-Chief Clause is a substantive grant of authority to the President. See, e.g., Memorandum for Charles W. Colson, Special Counsel to the President, from William H. Rehnquist, Assistant Attorney General, Office of Legal Counsel, *Re: The President and the War Power: South Vietnam and the Cambodian Sanctuaries* 5 (May 22, 1970) ("*Cambodian Sanctuaries*") ("[T]he designation of the President as Commander-in-Chief of the Armed Forces is a substantive grant of power."). It is thus well established in principle that the Clause provides some area of exclusive Executive authority beyond congressional control. The core of the Commander-in-Chief power is the authority to direct the armed forces in conducting a military campaign. Thus, the Supreme Court has made clear that the "President alone" is "constitutionally invested with the entire charge of hostile operations." *Hamilton v. Dillin*, 88 U.S. (21 Wall.) 73, 87 (1874); see also *United States v. Sweeney*, 157 U.S. 281, 284 (1895) ("[T]he object of the [Commander-in-Chief Clause] is evidently to vest in the President . . . such supreme and undivided command as would be necessary to the prosecution of a successful war." (emphasis added)); *The Federalist* No. 74, at 500 (Hamilton) ("Of all the cares or concerns of government, the direction of war most peculiarly demands those qualities which distinguish the exercise of power by a single hand. The direction of war implies the direction of the common strength; and the power of directing and employing the common strength, forms an usual and essential part in the definition of the executive authority."). Similarly, the Court has stated that, "[a]s commander-in-chief, [the President] is authorized to direct the movements of the naval and military forces placed by law at his command, and to employ them in the manner he may deem most effectual to harass and conquer and subdue the enemy." *Fleming v. Page*, 50 U.S. (9 How.) 603, 615 (1850). As Chief Justice Chase explained in 1866, Congress's power "extends to all legislation essential to the prosecution of war with vigor and success, except such as interferes with the command of the forces and the conduct of campaigns. That power and duty belong to the President as commander-in-chief." *Ex parte Milligan*, 71 U.S. (4 Wall.) 2, 139 (1866) (Chase, C.J., concurring) (emphasis added); cf. *Stewart v. Kahn*, 78 U.S. (11 Wall.) 493, 506 (1870) ("The measures to be taken in carrying on war . . . are not defined [in the Constitution]. The decision of all such questions rests wholly in the discretion of those to whom the substantial powers involved are confided by the Constitution."). (TS//SI-STELW//NF)

The President's authority, moreover, is at its height in responding to an attack upon the United States. As the Supreme Court emphasized in the *Prize Cases*, the President is "bound to resist force by force"; he need not await any congressional sanction to defend the Nation from attack and "[h]e must determine what degree of force the crisis demands." *The Prize Cases*, 67 U.S. (2 Black) 635, 668, 670 (1863). Based on such authorities, this Office has concluded that Congress has no power to interfere with presidential decisions concerning the actual management

~~TOP SECRET//COMINT-**[REDACTED]**STELLAR WIND-**[REDACTED]**/NOFORN~~

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

of a military campaign. See, e.g., Memorandum for Daniel J. Bryant, Assistant Attorney General, Office of Legislative Affairs, from Patrick Philbin, Deputy Assistant Attorney General, Office of Legal Counsel, *Re: Swift Justice Authorization Act 11-14* (Apr. 8, 2002); *Training of British Flying Students in the United States*, 40 Op. Att'y Gen. 58, 61 (1941) ("[I]n virtue of his rank as head of the forces, he has certain powers and duties with which Congress cannot interfere." (internal quotation marks omitted)).⁴⁰ As we have noted, "[i]t has never been doubted that the President's power as Commander-in-Chief authorizes him, and him alone, to conduct armed hostilities which have been lawfully instituted." *Cambodian Sanctuaries* at 15. And as we explained in detail above, see *supra* pp. 29-30, the interception of enemy communications is a traditional element of the conduct of such hostilities during wartime and necessarily lies at core of the President's Commander-in-Chief power. (~~TS//SI- STELW//NF~~)

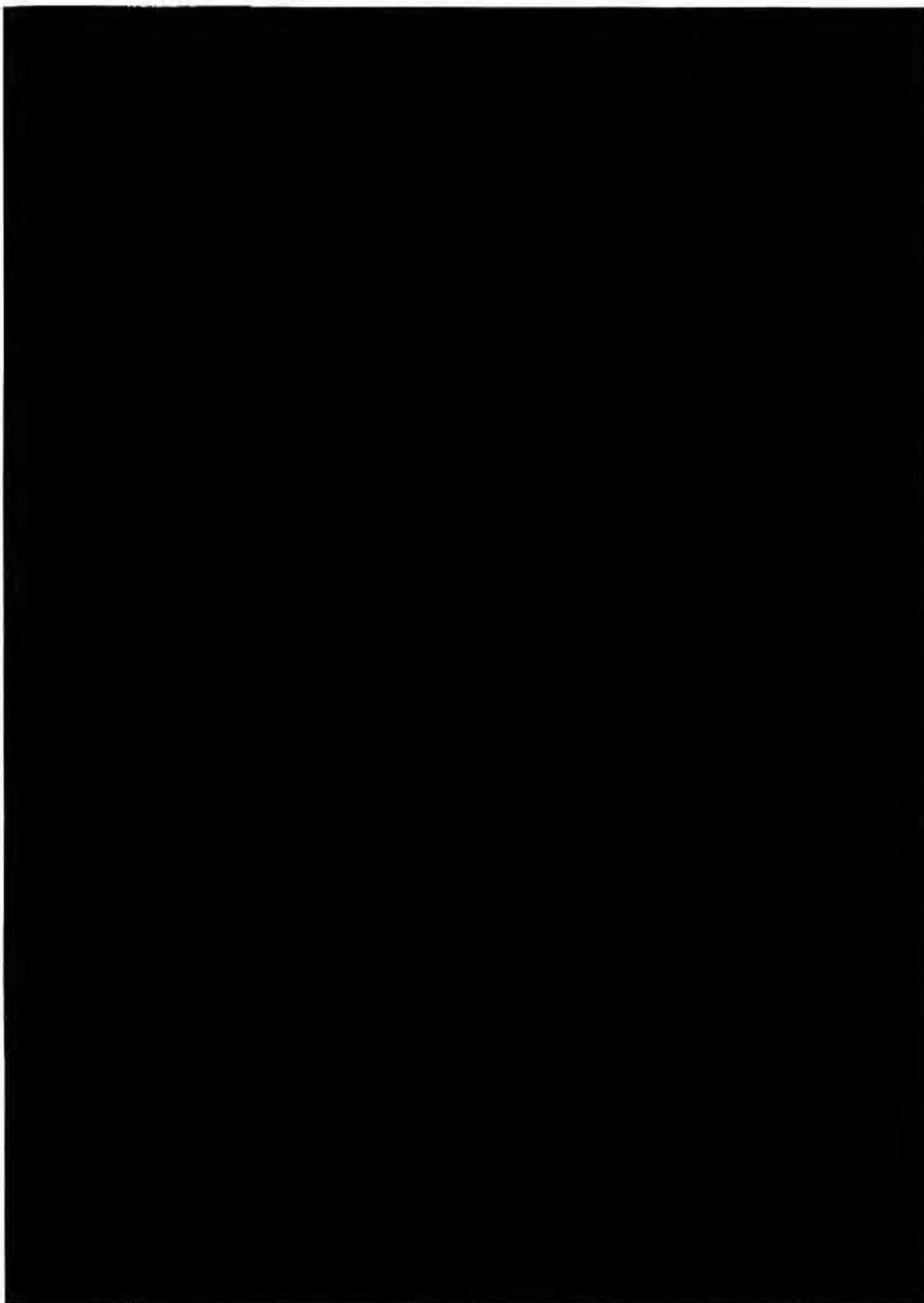
We believe that STELLAR WIND comes squarely within the Commander in Chief's authority to conduct the campaign against al Qaeda as part of the current armed conflict and that congressional efforts to prohibit the President's efforts to intercept enemy communications through STELLAR WIND would be an unconstitutional encroachment on the Commander-in-Chief power. (~~TS//SI- STELW//NF~~)



⁴⁰ Along similar lines, Francis Lieber, a principal legal adviser to the Union Army during the Civil War, explained that the "direction of military movement 'belongs to command, and neither the power of Congress to raise and support armies, nor the power to make rules for the government and regulation of the land and naval forces, nor the power to declare war, gives it the command of the army. Here the constitutional power of the President as commander-in-chief is exclusive.'" Clarence A. Berdahl, *War Powers of the Executive in the United States* 118 (1921) (quoting Lieber, *Remarks on Army Regulations* 18). (U)

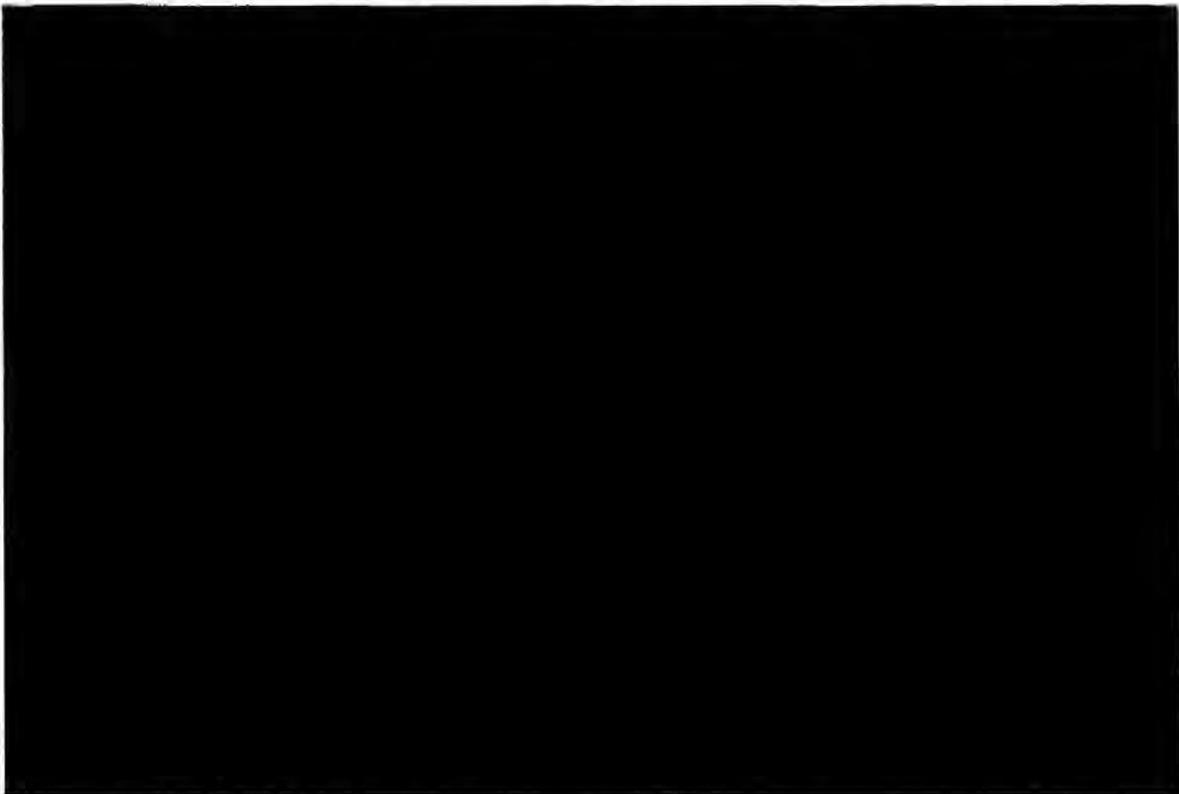
~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

~~TOP SECRET//~~ [REDACTED] ~~/COMINT- STELLAR WIND~~ [REDACTED] ~~//NOFORN~~



~~TOP SECRET//~~ [REDACTED] ~~/COMINT- STELLAR WIND~~ [REDACTED] ~~//NOFORN~~

~~TOP SECRET# [REDACTED] #COMINT- STELLAR WIND [REDACTED] #NOFORN~~



On the other side of the balance, there are instances in which executive practice has recognized some congressional control over the Executive's decisions concerning the armed forces. No example of which we are aware, however, involves an attempt at congressional regulation of the actual conduct of a campaign against enemy forces.⁴² For example, just before



⁴² Many have pointed to the annual message that President Thomas Jefferson sent to Congress in 1801 as support for the proposition that executive practice in the early days of the Republic acknowledged congressional power to regulate even the President's command over the armed forces. See, e.g., *Youngstown*, 343 U.S. at 64 n.10 (Jackson, J., concurring); Edward S. Corwin, *The President's Control of Foreign Relations* 131-33 (1917); Louis Fisher, *Presidential War Power* 25 (1995); see also Abraham D. Sofaer, *War, Foreign Affairs, and Constitutional Power: The Origins* 212 (1976) ("Most commentators have accepted this famous statement of deference to Congress as accurate and made in good faith."). In the message, Jefferson suggested that a naval force he had dispatched to the Mediterranean to answer threats to American shipping from the Barbary powers was "[u]nauthorized by the Constitution, without the sanction of Congress, to go beyond the line of defense." Sofaer, *War, Foreign Affairs, and Constitutional Power* at 212 (quoting 11 *Annals of Congress* 11-12). But the orders actually given to the naval commanders were quite different. They instructed the officers that, if upon their arrival

~~TOP SECRET# [REDACTED] #COMINT- STELLAR WIND [REDACTED] #NOFORN~~

~~TOP SECRET//COMINT-
STELLAR WIND//NOFORN~~

World War II, Attorney General Robert Jackson concluded that the Neutrality Act prohibited President Roosevelt from selling certain armed naval vessels (so-called "mosquito" boats) and sending them to Great Britain. See *Acquisition of Naval and Air Bases in Exchange for Over-Age Destroyers*, 39 Op. Att'y Gen. 484, 496 (1940). Thus, he concluded that Congress could control the Commander in Chief's ability to transfer that war materiel. That conclusion, however, does not imply any acceptance of direct congressional regulation of the Commander in Chief's control of the means and methods of engaging the enemy in an actual conflict. Indeed, Congress's authority in the context of controlling the sale of American naval vessels to another country was arguably bolstered in part by Congress's authority over "provid[ing] and maintain[ing] a Navy." U.S. Const. art. I, § 8, cl. 13. Similarly, in *Youngstown Sheet & Tube Co. v. Sawyer*, the Truman Administration readily conceded that, if Congress had by statute prohibited the seizure of steel mills, Congress's action would have been controlling. See Brief for Petitioner at 150, *Youngstown*, 343 U.S. 579 (1952) (Nos. 744 and 745) ("The President has made clear his readiness to accept and execute any Congressional revision of his judgment as to the necessary and appropriate means of dealing with the emergency in the steel industry."). There again, however, that concession concerning congressional control over a matter of economic production that might be related to the war effort implied no concession concerning control over the methods of engaging the enemy. (~~TS//SI-STLW//NF~~)

Lastly, in terms of executive authorities, there are many instances in which the Executive, after taking unilateral action in a wartime emergency, has subsequently sought congressional ratification of those actions. Most famously, President Lincoln sought congressional sanction in 1861 for having enlisted temporary volunteers in the army and having enlarged the regular army and navy while Congress was in recess. See *Message to Congress in Special Session* (July 4, 1861), in *Abraham Lincoln: Speeches and Writings, 1859-1865* at 252 (Don E. Fehrenbacher ed. 1989). In his proclamation ordering these actions, Lincoln explained that his orders would "be submitted to Congress as soon as assembled." *Proclamation of May 3, 1861*, 12 Stat. 1260. Such examples shed relatively little light, however, on the distinct question of Presidential authority to defy Congress. A decision to seek congressional support can be prompted by many motivations, including a desire for political support, and thus does not necessarily reflect any legal determination that Congress's power on a particular subject is paramount. In modern times, after all, several administrations have sought congressional authorizations for use of military force without conceding that such authorizations were in any way constitutionally required and while preserving the ability to assert the unconstitutionality of the War Powers Resolution. See, e.g., *Statement on Signing the Resolution Authorizing the Use of Military Force Against Iraq*, 1 Pub. Papers of George Bush 40 (1991) ("[M]y request for congressional support did not . . .

in the Mediterranean they should discover that the Barbary powers had declared war against the United States, "you will then distribute your force in such manner . . . so as best to protect our commerce and chastise their insolence - by sinking, burning or destroying their ships and vessels wherever you shall find them." *Id.* at 210 (quoting *Naval Documents Related to the United States War With the Barbary Powers* 465-67 (1939)); see also David P. Currie, *The Constitution in Congress: The Jeffersonians, 1801-1829* at 128 (2001) ("Neither the Administration's orders nor the Navy's actions reflected the narrow view of presidential authority Jefferson espoused in his Annual Message."); *id.* at 127 ("Jefferson's pious words to Congress were to a considerable extent belied by his own actions."). (U)

~~TOP SECRET//COMINT-
STELLAR WIND//NOFORN~~

TOP SECRET//COMINT- STELLAR WIND//NOFORN

constitute any change in the long-standing positions of the executive branch on either the President's constitutional authority to use the Armed Forces to defend vital U.S. interests or the constitutionality of the War Powers Resolution."'). Moreover, many actions for which congressional support has been sought – such as President Lincoln's action in raising an army in 1861 – quite likely do fall primarily under Congress's Article I powers. See U.S. Const. art. I, § 8, cl. 12 (granting Congress power "to raise and support Armies"). Again, however, such actions are readily distinguishable from the direct control over the conduct of a campaign against the enemy. Past practice in seeking congressional support in various other situations thus sheds little light on the precise separation of powers issue here. (TS//SI-STLW//NF)

There are two decisions of the Supreme Court that address a conflict between asserted wartime powers of the Commander in Chief and congressional legislation and that resolve the conflict in favor of Congress. They are *Little v. Barreme*, 6 U.S. (2 Cranch) 170 (1804), and *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952). These are the cases invariably cited by proponents of a congressional authority to regulate the Commander-in-Chief power. We conclude, however, that both are distinguishable from the situation presented by STELLAR WIND in the conflict with al Qaeda and thus that they do not support the constitutionality of the restrictions in FISA as applied here. (TS//SI-STLW//NF)

Barreme involved a libel brought to recover a ship seized by an officer of the United States Navy on the high seas during the Quasi War with France in 1799. The claimant sought return of the ship and damages from the officer on the theory that the seizure had been unlawful. The seizure had been based upon the officer's orders implementing an act of Congress suspending commerce between the United States and France. In essence, the orders from the President to the officer had directed him to seize any American ship bound *to* or *from* a French port. The ship in question was suspected of sailing *from* a French port. The statute on which the orders were based, however, had authorized solely the seizure of American ships bound *to* a French port. The Supreme Court concluded that the orders given by the President could not authorize a seizure beyond the terms of the statute – that is, they could not authorize anything beyond seizures of ships sailing *to* a French port. As the Court put it, "the legislature seem to have prescribed that the manner in which this law shall be carried into execution, was to exclude a seizure of any vessel not bound to a French port." *Id.* at 177-78 (emphasis omitted). As a result, the Court ruled not only that the seizure was not authorized, but also that the officer was liable in damages, despite having acted within his orders. See *id.* at 178-79. The decision has been broadly characterized by some as one in which the Court concluded that Congress could restrict by statute the means by which the President as Commander in Chief could direct the armed forces to carry on a war. See, e.g., Glennon, *Constitutional Diplomacy* at 13 ("In *Little* . . . , an implied congressional prohibition against certain naval seizures prevailed over the President's constitutional power as commander-in-chief." (footnote omitted)); *Foreign and Military Intelligence, Book I: Final Rep. of the Senate Select Comm. to Study Gov'tal Operations with Respect to Intelligence Activities*, S. Rep. No. 94-755, at 39 (1976) (characterizing *Barreme* as "affirm[ing]" the "constitutional power of Congress" to limit "the types of seizures that could be made" by the Navy); cf. Henry P. Monaghan, *The Protective Power of the Presidency*, 93

TOP SECRET//COMINT- STELLAR WIND//NOFORN

~~TOP SECRET// [REDACTED] /COMINT- STELLAR WIND [REDACTED] /NOFORN~~

Colum. L. Rev. 1, 24-25 (1993) (arguing that *Barreme* establishes the principle that the President has no authority to act "contra legem, even in an emergency"). (TS//SI-STLW//NF)

We think such a characterization greatly overstates the scope of the decision, which is limited in three substantial ways. First, the operative section of the statute in question restricted the movements of and granted authority to seize *American* merchant ships.⁴³ It was not a provision that purported to regulate by statute the steps the Commander in Chief could take in confronting armed vessels of the *enemy*. Thus, neither in *Barreme* nor in any other case arising from the Quasi War (so far as we are aware) did the Supreme Court have occasion to rule on whether, even in the limited and peculiar circumstances of the Quasi War, Congress could have placed some restriction on the orders the Commander in Chief could issue concerning direct engagements with enemy forces.⁴⁴ We think that distinction is particularly important when the content collection aspect of STELLAR WIND is under consideration, because content collection is directed solely against targeted telephone numbers or e-mails where there is a reason for believing that one of the communicants is an enemy. (TS//SI-STLW//NF)

Second, and relatedly, it is significant that the statute in *Barreme* was expressly cast, not as a limitation on the conduct of warfare, but rather as a measure on a subject within the core of Congress's responsibilities under Article I – regulating foreign commerce. See *supra* n.43

⁴³ The text of the first section of the act provided that "from and after the first day of March next no ship or vessel owned, hired or employed, wholly or in part, by any person resident within the United States, and which shall depart there from, shall be allowed to proceed directly, or from any intermediate port or place, to any port or place within the territory of the French republic." *Barreme*, 6 U.S. (2 Cranch) at 170 (quoting Act of February 9, 1799) (emphases omitted). Section 5 provided "[t]hat it shall be lawful for the President of the United States, to give instructions to the commanders of the public armed ships of the United States, to stop and examine any ship or vessel of the United States, on the high sea, which there may be reason to suspect to be engaged in any traffic or commerce contrary to the true tenor hereof; and if, upon examination, it shall appear that such ship or vessel is bound or sailing to any port or place within the territory of the French republic, or her dependencies, contrary to the intent of this act, it shall be the duty of the commander of such public armed vessel, to seize every such ship or vessel engaged in such illicit commerce . . ." *Id.* at 171 (emphases omitted). (U)

⁴⁴ In fact, if anything the one case that came close to raising such a question tends to suggest that the Court would not have upheld such a restriction. In that case the Court was careful to construe the statutes involved so as not to restrict the ability of the armed vessels of the United States to engage armed vessels under French control. In *Talbot v. Seeman*, 5 U.S. (1 Cranch) 1 (1801), the *U.S.S. Constitution* had captured an armed merchant vessel, the *Amelia*, that, although originally under a neutral flag, had previously been captured and manned by a prize crew from the French navy. The Court explained that, under the statutes then in force, there was no law authorizing a public armed vessel of the United States to capture such a vessel because, technically, in contemplation of law it was still a neutral vessel until the French prize crew had brought it to port and had it formally adjudicated a lawful prize. See *id.* at 30-31. The Court concluded that the capture was lawful, however, because the captain of the *Constitution* had probable cause at the time of the capture to doubt the character of the ship. The Court went on to explain, moreover, that even if "the character of the *Amelia* had been completely ascertained," the capture still would have been lawful because "as she was an armed vessel under French authority, and in a condition to annoy the American commerce, it was [the American captain's] duty to render her incapable of mischief." *Id.* at 32. The Court reached that conclusion even though there was also no act of Congress authorizing public armed vessels of the United States to seize such vessels under French control. The Court concluded that the statutes must nevertheless be construed to permit, and certainly not to prohibit, such an action. *Id.* at 32-33. (U)

~~TOP SECRET// [REDACTED] /COMINT- STELLAR WIND [REDACTED] /NOFORN~~

~~TOP SECRET//COMINT//STELLAR WIND//NOFORN~~

(quoting text of Act of February 9, 1799). It happened that many of the actions taken by the armed forces during the Quasi War involved solely enforcing restrictions such as that contained in the statute in *Barreme*. But that was part and parcel of the peculiar and limited nature of the war that gave it its name. The measures that Congress imposed restricting commerce took center stage in the "conflict" because the extent of full-blown hostilities between the armed forces was extremely limited. See Alexander DeConde, *The Quasi-War* 126 (1966) ("The laws themselves were half measures . . . , were basically defensive, and were to expire when the commanders of French ships stopped their depredations against American commerce. This was why, from the American point of view, the clash with France was a quasi-war."). (TS//SI//STLW//NF)

Finally, reviewing *Barreme* in light of both contemporary decisions addressing the nature of the conflict with France and later precedents, such as the *Prize Cases*, 67 U.S. (2 Black) 635 (1863), makes clear that the Supreme Court considered the unusual and limited nature of the maritime "war" with France a critical factor in concluding that statutes might constrain the Commander in Chief's directives to the armed forces. The Court's decision was fundamentally based on the premise that the state of affairs with France was not sufficiently akin to a full-scale war for the President to invoke under his own inherent authority the full rights of war that, in other cases, he might have at his disposal. As a result, he required the special authorization of Congress to act. The opinion of the lower court in the case, which is quoted at length in the report of the Supreme Court decision, makes this premise clear. As the lower court had explained: "If a war of a common nature had existed between the United States and France, no question would be made but the false papers found on board, the destruction of the log-book and other papers, would be a sufficient excuse for the capture, detention and consequent damages. It is only to be considered whether the same principles as they respect neutrals are to be applied to this case." *Id.* at 173 (emphasis omitted). (TS//SI//STLW//NF)

The opinion of the Supreme Court, delivered by Chief Justice Marshall, echoes the same principle. In framing his discussion, Chief Justice Marshall made clear that "[i]t is by no means clear that the president of the United States whose high duty it is to 'take care that the laws be faithfully executed,' and who is commander in chief of the armies and navies of the United States, might not, without any special authority for that purpose, in the then existing state of things, have empowered the officers commanding the armed vessels of the United States, to seize and send into port for adjudication, American vessels which were forfeited by being engaged in this illicit commerce." *Id.* at 177. In other words, "in the then existing state of things" there was not a sufficiently clear state of war that the President might have exercised the rights of war to stop and examine the vessel and interdict commerce with the enemy. Instead, he required "special authority for that purpose." But if he required "special authority" from Congress, the extent of that authority could necessarily be limited by whatever restrictions Congress might impose. Of course, because the Court viewed "the then existing state of things" as insufficient for the President to invoke the rights of war under his own inherent authority, the Court had no occasion to address the power of Congress to limit the Commander in Chief's authority in such a case. (TS//SI//STLW//NF)

~~TOP SECRET//COMINT//STELLAR WIND//NOFORN~~

TOP SECRET// [REDACTED] //COMINT- STELLAR WIND [REDACTED] //NOFORN

This understanding is buttressed by contemporary decisions addressing other actions in the Quasi War. Such decisions make it clear, for example, that the Court considered the limited character of the war a peculiar state of affairs in international law. As Justice Moore explained four years earlier in *Bas v. Tingy*, 4 U.S. (4 Dall.) 37 (1800), "our situation is so extraordinary, that I doubt whether a parallel case can be traced in the history of nations." *Id.* at 39 (Moore, J.). Members of the Court also indicated their understanding that a more "perfect" state of war in itself could authorize the Executive to exercise the rights of war, because in such a war "its extent and operations are only restricted and regulated by the *jus belli*, forming a part of the law of nations." *Id.* at 44, 43 (Chase, J.). Indeed, the very same distinction between a full-fledged state of war (which would inherently authorize the President to invoke the rights of war as recognized under the law of nations) and a more qualified state of hostilities (where congressional authorization would be necessary) was also discussed, although it was not central to the holding, in *Bas v. Tingy*. The critical issue in the case was whether a particular statute defining the rights of salvage and the portions to be paid for salvage applied to a friendly vessel recaptured from the French, or whether its application was more restricted in time. Justice Washington explained his view that the law should apply "whenever such a war should exist between the United States and France, or any other nation, as according to the law of nations, or special authority, would justify the recapture of friendly vessels." *Id.* at 41-42 (Washington, J.). That phrasing clearly reflects the assumption that the recapture of a vessel might be authorized either by the type of war that existed in itself or by "special authority" provided by Congress. Similarly, Justice Washington went on to explain that in another case he had concluded as circuit justice that "neither the *sort of war that subsisted*, nor the special commission under which the American acted, authorised" the capture of a particular vessel. *Id.* at 42 (emphases altered). Again, this analysis reflects the assumption that the Quasi War was not the "sort of war" that permitted the Executive to exercise the full rights of war under the Commander in Chief's inherent authority, but that such wars could arise. Given the limited nature of the Quasi War, of course, in *Bas* the Court had no occasion to consider the question whether Congress might restrict the Commander in Chief's orders to the navy in a situation where the "sort of war that subsisted" would have allowed the President on his own authority to invoke the full rights of war under the law of nations. (TS//SI-STLW//NF)

Understood in this light, it seems clear that in the Supreme Court's view, *Barreme* did not involve a situation in which there was a sufficiently full-scale war that would, in and of itself, suffice to trigger the powers of the President as Commander in Chief to direct the armed forces in a campaign. And thus the Court had no occasion to consider whether Congress might by statute restrict the President's power to direct the armed forces as he might see fit in such a conflict. Much less did the Court consider in *Barreme* the situation where a full-scale war was initiated by a foreign attack – a situation in which, as the Court later made clear in the *Prize Cases*, the President would need no special authority from Congress: "If a war be made by invasion of a foreign nation, the President is not only authorized but bound to resist force by force. He does not initiate the war, but is bound to accept the challenge without waiting for any special legislative authority." 67 U.S. (2 Black) at 668. (TS//SI-STLW//NF)

TOP SECRET// [REDACTED] //COMINT- STELLAR WIND [REDACTED] //NOFORN

TOP SECRET// [REDACTED] /COMINT- STELLAR WIND [REDACTED] //NOFORN

The limited nature of the conflict at issue in *Barre* distinguishes it from the current state of armed conflict between the United States and al Qaeda. This conflict has included a full-scale attack on the United States that killed thousands of civilians and precipitated an unprecedentedly broad Congressional Authorization for the Use of Military Force followed by major military operations by U.S. armed forces that continue to this day. (TS//SI-STLW//NF)

The second Supreme Court decision that involves a direct clash between asserted powers of the Commander in Chief and Congress is *Youngstown*. Some commentators have invoked the holding in *Youngstown* and the analysis in Justice Jackson's concurrence to conclude that, at least when it occurs within the United States, foreign intelligence collection is an area where the Legislative and Executive branches share concurrent authority and that Congress may by statute comprehensively regulate the activities of the Executive. See, e.g., David S. Egger, Note, *Executive Order 12,333: An Assessment of the Validity of Warrantless National Security Searches*, 1983 Duke L. J. 611, 636-37; cf. John Norton Moore et al., *National Security Law* 1025 (1990). The case is also routinely cited more broadly as an affirmation of Congress's powers even in the face of claims by the Commander in Chief in wartime. It is true that *Youngstown* involved a situation in which the Executive, relying *inter alia* on the Commander-in-Chief power, attempted to take action that Congress had apparently foreclosed by statute, and that the Supreme Court held the executive action invalid. Beyond a superficial parallel at that level of generality, however, we do not think the analogy to *Youngstown* is apt. (TS//SI-STLW//NF)

Youngstown involved an effort by the President -- in the face of a threatened work stoppage -- to seize and run steel mills. Steel was a vital resource for manufacturers to produce the weapons and other materiel that were necessary to support troops overseas in Korea. See 343 U.S. at 582-84. In drafting the Labor Management Relations Act of 1947 (also known as the Taft-Hartley Act) Congress had expressly considered the possibility of giving the President the power to effect such a seizure of industry in a time of national emergency. It had rejected that option, however, and instead provided different mechanisms for resolving labor disputes. See *id.* at 586. Other statutes, moreover, did provide certain mechanisms for seizing industries to ensure production vital to national defense. See *id.* at 585-86 & n.2. President Truman, however, chose not to follow any of these mechanisms and instead asserted inherent authority to seize the mills to ensure the production of steel. (TS//SI-STLW//NF)

The Court rejected the President's assertion of powers under the Commander-in-Chief Clause primarily because the connection between the President's action and the core Commander-in-Chief function of commanding the armed forces was simply too attenuated. As the Court pointed out, "[e]ven though 'theater of war' [may] be an expanding concept," the case clearly did not involve the authority over "day-to-day fighting in a theater of war." *Id.* at 587. Instead, it involved a dramatic extension of the President's authority from control over military operations to control over an industry that was vital for supplying other industries that in turn produced items vital for the forces overseas. The almost limitless implications of the theory behind President Truman's approach -- which could potentially permit the President unilateral authority to control any sector of the economy deemed vital to a war effort -- was clearly an

TOP SECRET// [REDACTED] /COMINT- STELLAR WIND [REDACTED] //NOFORN

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

important factor influencing the Court's decision. Indeed, Justice Jackson's influential concurring opinion reveals a clear concern for what might be termed foreign-to-domestic presidential bootstrapping. The United States became involved in the Korean conflict through President Truman's unilateral decision, without consulting Congress, to commit U.S. troops to the defense of South Korea when the North invaded in 1950. That was a national security and foreign policy decision to involve U.S. troops in a wholly foreign war. In *Youngstown*, the President was claiming authority, based upon that foreign war, to extend far-reaching presidential control into vast sectors of the domestic economy. Justice Jackson expressed "alarm[]" at a theory under which "a President whose conduct of foreign affairs is so largely uncontrolled, and often even is unknown, can vastly enlarge his mastery over the internal affairs of the country by his own commitment of the Nation's armed forces to some foreign venture." *Id.* at 642 (Jackson, J., concurring). (FS//SI-STLW/NF)

Critically, moreover, President Truman's action involved extending the Executive's authority into a field where the Constitution had assigned Congress, in the ordinary case, a preeminent role. As the majority explained, under the Commerce Clause, Congress "can make laws regulating the relationships between employers and employees, prescribing rules designed to settle labor disputes, and fixing wages and working conditions in certain fields of our economy. The Constitution did not subject this law-making power of Congress to presidential or military supervision or control." *Id.* at 588; *see also id.* at 587 ("This is a job for the Nation's lawmakers, not for its military authorities."). In addition, as Justice Jackson pointed out in concurrence, Congress is also given express authority to "'raise and support Armies'" and "'to provide and maintain a Navy.'" *Id.* at 643 (Jackson, J., concurring) (quoting U.S. Const. art. 1, § 8, cls. 12, 13). These grants of authority seemed to give "Congress primary responsibility for supplying the armed forces," *id.*, and the crisis at hand involved a matter of supply. Thus, *Youngstown* involved an assertion of executive power that not only stretched far afield from core Commander-in-Chief functions, but that did so by intruding into areas where Congress had been given an express, and likely dominant, role by the Constitution. (FS//SI-STLW/NF)

The situation here presents a very different picture. First, the exercise of executive authority here is not several steps removed from the actual conduct of a military campaign. To the contrary, content collection under STELLAR WIND is an intelligence operation undertaken by the Department of Defense specifically to detect operational communications of enemy forces that will enable the United States to detect and disrupt planned attacks, largely by detecting enemy agents already within the United States. Al Qaeda has already demonstrated an ability, both on September 11 and subsequently (in cases such as Jose Padilla and Ali al-Marri⁴⁵) to insert agents into the United States. As explained above, the efforts under STELLAR WIND to intercept communications that would lead to the discovery of more such agents or other planned

⁴⁵ Al-Marri entered the United States on September 10, 2001. He was originally "detained in December 2001 as a material witness believed to have evidence about the terrorist attacks of September 11," and the President later determined he is "an enemy combatant affiliated with al Qaeda." *Al-Marri v. Rumsfeld*, 360 F.3d 707, 708 (7th Cir. 2004). (U)

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

~~TOP SECRET// [REDACTED] //COMINT- STELLAR WIND [REDACTED] //NOFORN~~

attacks on the United States are a core exercise of Commander-in-Chief authority in the midst of an armed conflict. (TS//SI-STLW//NF)

In addition, the theme that appeared most strongly in Justice Jackson's concurrence in *Youngstown* expressing a concern for a form of presidential boot-strapping simply does not apply in this context. Justice Jackson evinced a concern for two aspects of what might be termed boot-strapping in the Executive's position in *Youngstown*. First, the President had used his own inherent constitutional authority to commit U.S. troops to the Korean conflict. He was then attempting, without any express authorization for the conflict from Congress, to expand his authority further on the basis of the need to support the troops already committed to hostilities. Here, however, Congress expressly provided the President sweeping authority immediately after September 11, 2001 to use "all necessary and appropriate force" as he deemed required to protect the Nation from further attack. Congressional Authorization § 2(a). Second, in *Youngstown* Justice Jackson was concerned that the President was using an exercise of his Commander-in-Chief powers in the foreign realm to justify his assumption of authority over domestic matters within the United States. Again, this concern must be understood in light of both the particular context of the Korean conflict and the type of powers being asserted. There, the conflict was strictly confined to the Korean peninsula overseas, and there was no suggestion that the President's actions in the United States had any connection whatsoever to meeting an enemy threat *within the United States*. As a result, *Youngstown* must not be overread to suggest that the President's authorities for engaging the enemy are necessarily somehow less extensive inside the United States than they are abroad. The extent of the President's authorities will necessarily depend on where the enemy is found. Long before *Youngstown*, it was recognized that, in a large-scale conflict, the area of operations could readily extend to the continental United States, even when there are no major engagements of armed forces here. As long ago as 1920 in the context of the trial of a German officer for spying in World War I, it was recognized that "[w]ith the progress made in obtaining ways and means for devastation and destruction, the territory of the United States was certainly within the field of active operations" during the war, particularly in the port of New York, and that a spy in the United States might easily have aided the "hostile operations" of U-boats off the coast. *United States ex rel. Wessels v. McDonald*, 265 F. 754, 764 (E.D.N.Y. 1920). Similarly, in World War II, in *Ex parte Quirin*, 317 U.S. 1 (1942), the Supreme Court readily recognized that the President had authority as Commander in Chief to capture and try agents of the enemy in the United States, and indeed that he could do so even if they had never "entered the theatre or zone of active military operations." *Id.* at 38.⁴⁶ (TS//SI-STLW//NF)

In this conflict, moreover, the battlefield was brought to the United States in the most literal way on September 11, 2001, and ongoing intelligence indicates that further attacks on the United States will be attempted. In addition, in this conflict, precisely because the enemy

⁴⁶ But see *Padilla v. Runsfeld*, 352 F.3d 695, 712 (2d Cir. 2003) (holding that an al Qaeda operative seized in Chicago could not be detained in South Carolina without statutory authorization because "the President lacks inherent constitutional authority as Commander-in-Chief to detain American citizens on American soil outside a zone of combat"), *cert. granted*, 124 S. Ct. 1353 (2004). (U)

~~TOP SECRET// [REDACTED] //COMINT- STELLAR WIND [REDACTED] //NOFORN~~

TOP SECRET// [REDACTED] //COMINT- STELLAR WIND [REDACTED] //NOFORN

operates by stealth and seeks to infiltrate the United States undetected, it is the intelligence front that is the most vital aspect of the battle for protecting America. Thus, while some justices in *Youngstown* expressed concern at the President's efforts to claim Commander-in-Chief powers for actions taken in the United States, that concern must be understood in the context of a conflict that was limited wholly to foreign soil. The North Koreans in 1950 had no ability to project force against the continental United States and the Court in *Youngstown* was not confronted with such a concern. Al Qaeda, by contrast, has demonstrated itself more successful at projecting force against the mainland United States than any foreign enemy since British troops burned Washington, D.C., in the War of 1812. There is certainly nothing in *Youngstown* to suggest that the Court would not agree that, after an attack such as September 11, American soil was most emphatically part of the battle zone and that the President's Commander-in-Chief powers would fully apply to seek out, engage, and defeat the enemy – even in the United States. Similarly, there is certainly no question of presidential bootstrapping from a "foreign venture" here. This conflict was thrust upon the Nation by a foreign attack carried out directly on American soil.
(TS//SI-STLW//NF)

Finally, an assertion of executive authority here does not involve extending presidential power into spheres ordinarily reserved for Congress. To the contrary, as outlined above, congressional authority in this field is hardly clear.

[REDACTED]

(TS//SI-STLW//NF)

In short, we do not think that *Youngstown* provides any persuasive precedent suggesting that Congress may constitutionally prohibit the President from engaging in the activities contemplated in STELLAR WIND. (TS//SI-STLW//NF)

[REDACTED]

TOP SECRET// [REDACTED] //COMINT- STELLAR WIND [REDACTED] //NOFORN

Pages 65 – 68
Withheld in Full

JA335

OLC 074

~~TOP SECRET~~ [REDACTED] ~~/COMINT-STELLAR WIND~~ [REDACTED] ~~/NOFORN~~

[REDACTED]

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

[REDACTED]

Taking into account all the considerations outlined above, we conclude that the signals intelligence activity undertaken to collect the content of enemy communications under

[REDACTED]

~~TOP SECRET~~ [REDACTED] ~~/COMINT-STELLAR WIND~~ [REDACTED] ~~/NOFORN~~

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

STELLAR WIND comes within the core powers of the Commander in Chief in conducting a military campaign and that provisions in FISA or Title III that would prohibit it are unconstitutional as applied. It is critical to our conclusion that the issue arises in the context of a war instituted by an attack on the United States and necessitating the use of the armed forces to defend the Nation from attack. That brings this situation into the core of the President's Commander-in-Chief powers. It has long been recognized that the President has extensive unilateral authority even to initiate armed action to protect American lives abroad. *See, e.g., Durand v. Hollins*, 8 F. Cas. 111, 112 (C.C.S.D.N.Y. 1860) (No. 4186). If anything, we believe that power is greater when the Nation itself is under attack. It is fortunate that in our history the courts have not frequently had occasion to address the powers of the President in responding to such aggression. In the one precedent most squarely on point, however, the Supreme Court made abundantly clear that his authority is broad indeed. As the Court put it in the *Prize Cases*, "[i]f war be made by invasion of a foreign nation, the President is not only authorized but bound to resist force by force," 67 U.S. (2 Black) at 668, and "[h]e must determine what degree of force the crisis demands," *id.* at 670. It is true that the Court had no occasion there to consider the relative powers of Congress and the President if they should come into conflict. Nevertheless, the Court's language in the *Prize Cases* suggests that if there is any area that lies at the core of the Commander in Chief's power, it is actions taken directly to engage the enemy in protecting the Nation from an attack. In this regard, it bears emphasis that the obligation to "protect each of [the States] against invasion" is one of the few affirmative obligations the Constitution places on the federal government with respect to the States. U.S. Const. art. IV, § 4. It is primarily the President, moreover, who must carry out that charge. Indeed, defense of the Nation is an aspect of the explicit oath of office that the Constitution prescribes for the President, which states that the President shall "'to the best of [his] Ability, preserve, protect and defend the Constitution of the United States.'" U.S. Const. art. II, § 1. Here, we conclude that the content collection activities under STELLAR WIND are precisely a core exercise of Commander-in-Chief powers to detect and engage the enemy in protecting the Nation from attack in the midst of a war and that Congress may not by statute restrict the Commander in Chief's decisions about such a matter involving the conduct of a campaign. (TS//SI-STLW//NF)

Even if we did not conclude that STELLAR WIND was within the core of the Commander-in-Chief power with which Congress cannot interfere, we would conclude that the restrictions in FISA would frustrate the President's ability to carry out his constitutionally assigned functions as Commander in Chief and are impermissible on that basis. As noted above, even in prior opinions suggesting that Congress has the power to restrict the Executive's actions in foreign intelligence collection this Office has always preserved the caveat that such restrictions would be permissible only where they do not "go so far as to render it impossible for the President to perform his constitutionally prescribed functions." [REDACTED] Several factors combine to make the FISA process an insufficient mechanism for responding to the crisis the President has faced in the wake of the September 11 attacks. (TS//SI-STLW//NF)

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

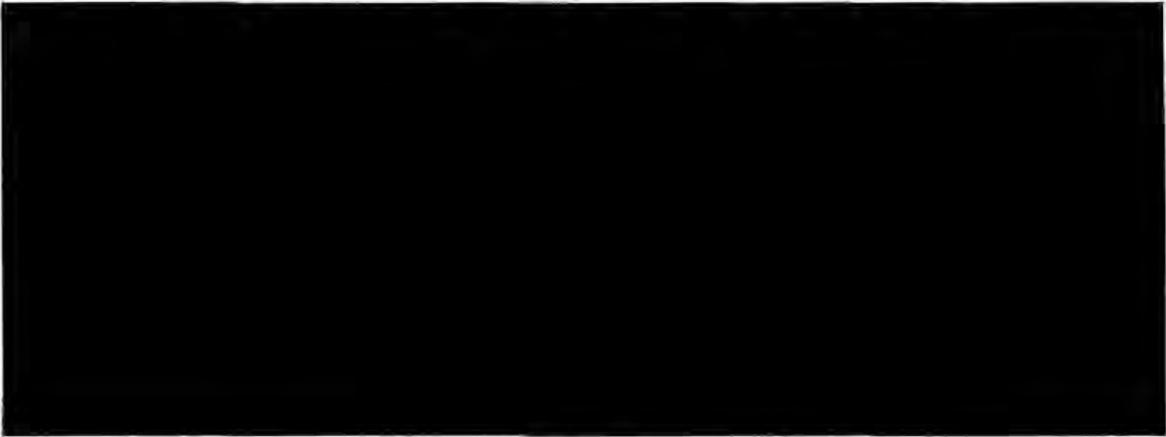
Pages 71 – 73

Withheld in Full

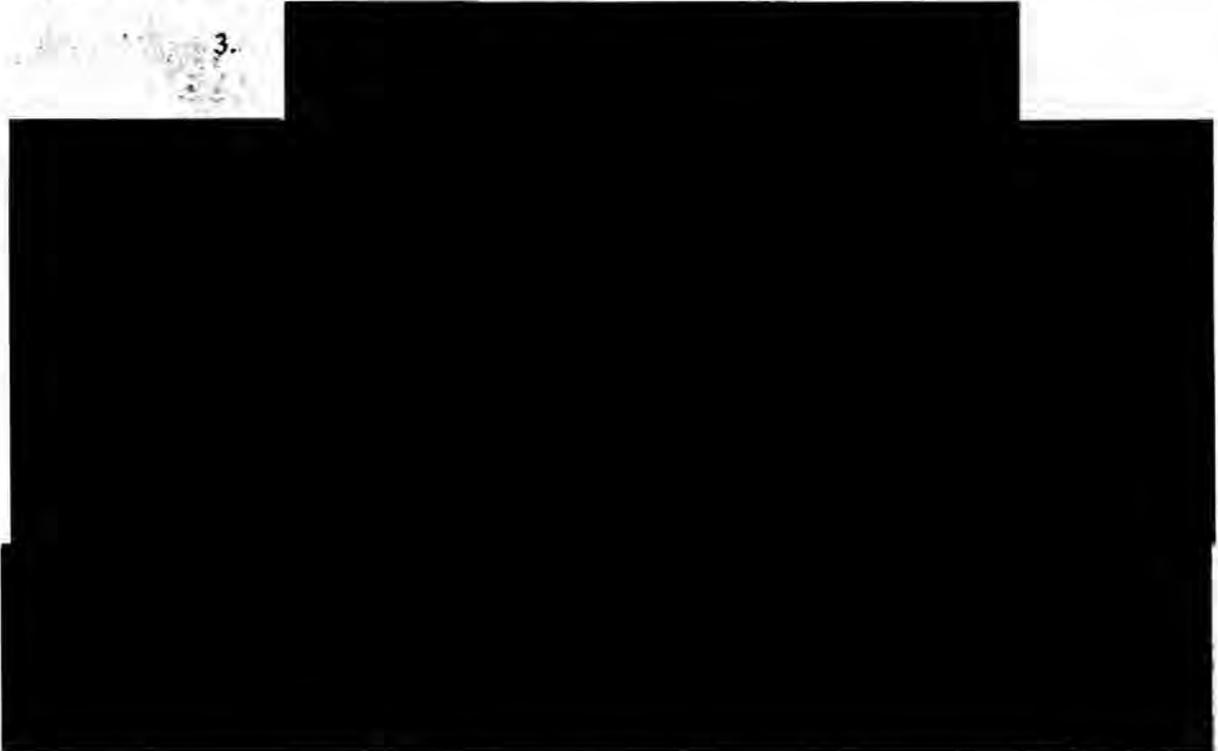
JA338

OLC 077

TOP SECRET//~~COMINT-STELLAR WIND~~//NOFORN



To summarize, we conclude only that when the Nation has been thrust into an armed conflict by a foreign attack on the United States and the President determines in his role as Commander in Chief and sole organ for the Nation in foreign affairs that it is essential for defense against a further foreign attack to use the signals intelligence capabilities of the Department of Defense within the United States, he has inherent constitutional authority to direct electronic surveillance without a warrant to intercept the suspected communications of the enemy – an authority that Congress cannot curtail. We need not, and do not, express any view on whether the restrictions imposed in FISA are a constitutional exercise of congressional power in circumstances of more routine foreign intelligence gathering that do not implicate an armed conflict and direct efforts to safeguard the Nation from a credible danger of foreign attack.
(TS//SI STELW//NF)

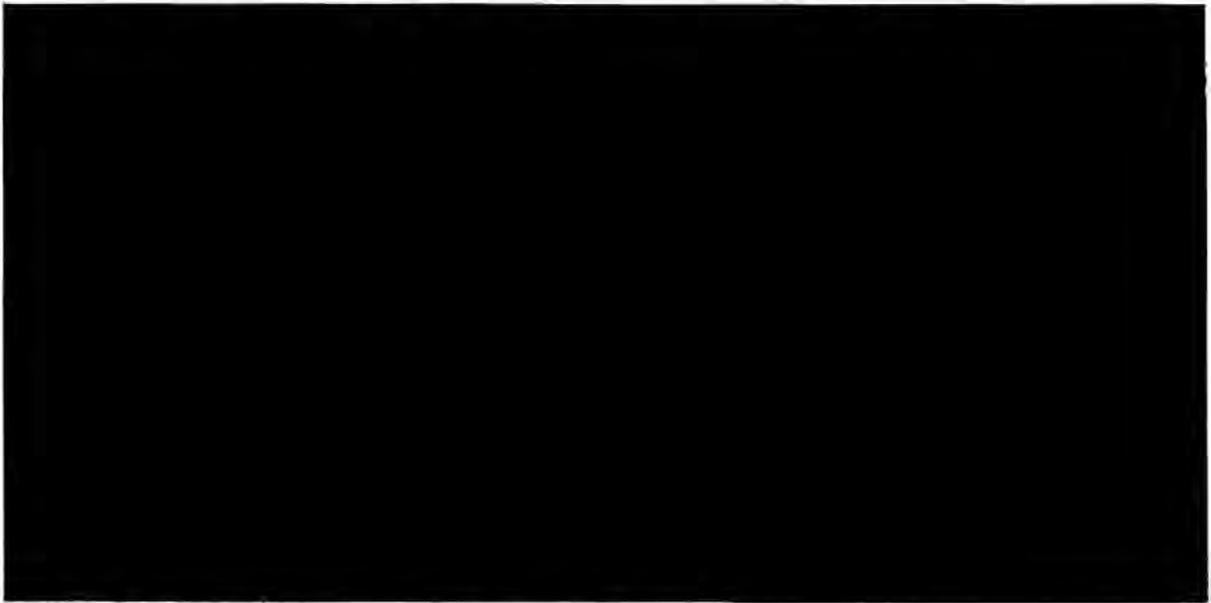


TOP SECRET//~~COMINT-STELLAR WIND~~//NOFORN

Pages 75 – 80

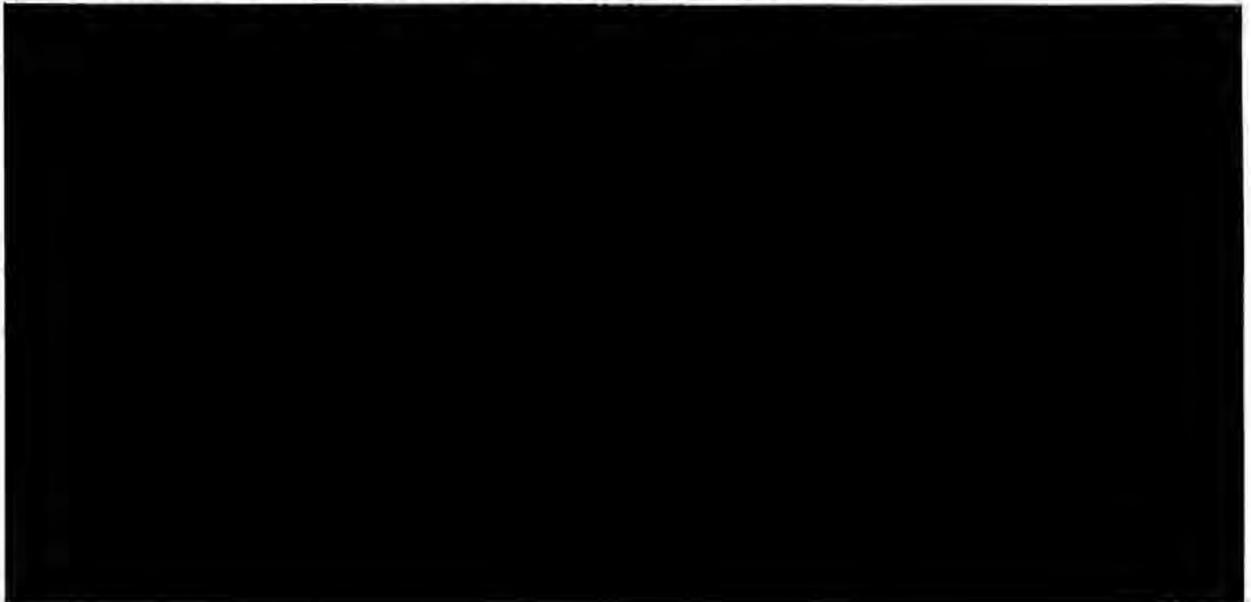
Withheld in Full

~~TOP SECRET// [REDACTED]//COMINT- STELLAR WIND [REDACTED]//NOFORN~~



III. Telephony Dialing-Type Meta Data Collection – Statutory Analysis
(TS//SI- STLW//NF)

The second major aspect of the STELLAR WIND program as it is currently operated is the collection of telecommunications dialing-type data [REDACTED]. This data, known as "meta data," does not include the content of communications. Rather, it consists essentially of the telephone number of the calling party, the telephone number of the called party, and the date, time, and duration of the telephone call. For ease of reference, we will refer to this aspect of STELLAR WIND as meta data collection. (TS//SI- STLW//NF)



~~TOP SECRET// [REDACTED]//COMINT- STELLAR WIND [REDACTED]//NOFORN~~

Pages 82 – 99

Withheld in Full

JA342

OLC 081

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

V. STELLAR WIND Under the Fourth Amendment (~~TS//SI-STLW//NF~~)

The analysis above establishes that the constraints imposed by FISA and title 18 that would seem to prohibit the activities undertaken in STELLAR WIND are either best construed to have been superseded by the Congressional Authorization for Use of Military Force, or, if applicable, are unconstitutional as applied in this context.

The final step in our analysis requires an examination of STELLAR WIND under the Fourth Amendment. (~~TS//SI-STLW//NF~~)

In determining the scope of executive power to conduct foreign intelligence searches, we have already concluded above that there is an exception to the Fourth Amendment's warrant requirement for such searches. See Part II.C.1, *supra*. For that analysis, we assumed that some activities undertaken under STELLAR WIND would be subject to the Fourth Amendment. It remains for us now to turn to a more comprehensive examination of STELLAR WIND under the Fourth Amendment. Once again, we divide our analysis to address separately (i) interception of the content of communications and (ii) the acquisition of meta data. (~~TS//SI-STLW//NF~~)

We recognize that there may be a sound argument for the proposition that the Fourth Amendment does not even apply to a military operation such as STELLAR WIND.⁸⁴ Assuming *arguendo*, however, that it does apply, we analyze STELLAR WIND's content interceptions under the Fourth Amendment standard of reasonableness. As the Supreme Court has explained, this analysis requires a balancing of the governmental interest at stake against the degree of

⁸⁴ See, e.g., Memorandum for Alberto R. Gonzales, Counsel to the President, and William J. Haynes, II, General Counsel, Department of Defense, from John C. Yoo, Deputy Assistant Attorney General, and Robert J. Delahunty, Special Counsel, Office of Legal Counsel, *Re: Authority for Use of Military Force To Combat Terrorist Activities Within the United States* 25 (Oct. 23, 2001) ("In light of the well-settled understanding that constitutional constraints must give way in some respects to the exigencies of war, we think that the better view is that the Fourth Amendment does *not* apply to domestic military operations designed to deter and prevent further terrorist attacks."). (U)

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

~~TOP SECRET//COMINT-**[REDACTED]**STELLAR WIND**[REDACTED]**/NOFORN~~

intrusion into protected areas of privacy. See, e.g., *Board of Educ. v. Earls*, 536 U.S. 822, 829 (2002) (“[W]e generally determine the reasonableness of a search by balancing the nature of the intrusion on the individual’s privacy against the promotion of legitimate governmental interests.”). Under that balancing, we conclude that the searches at issue here are reasonable. (TS//SI-STLW//NF)

As for meta data collection, as explained below, we conclude that under the Supreme Court’s decision in *Smith v. Maryland*, 442 U.S. 735 (1979), the interception of the routing information for both telephone calls and e-mails does not implicate any Fourth Amendment interests.⁸⁵ (TS//SI-STLW//NF)

A. **STELLAR WIND Content Interceptions Are Reasonable Under Balancing-of-Interests Analysis** (TS//SI-STLW//NF)

Under the standard balancing of interests analysis used for gauging reasonableness, the STELLAR WIND interceptions would pass muster under the Fourth Amendment. As the Supreme Court has emphasized repeatedly, “[t]he touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined by assessing, on the one hand, the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.” *United States v. Knights*, 534 U.S. 112, 118-19 (2001). The Court has found a search reasonable when, under the totality of the circumstances, the “importance of the governmental interests” has outweighed the “nature and quality of the intrusion on the individual’s Fourth Amendment interests.” *Tennessee v. Garner*, 471 U.S. 1, 8 (1985). (TS//SI-STLW//NF)

We begin by addressing the individual privacy interests at stake. There can be no doubt that, as a general matter, interception of the content of telephone communications implicates a significant privacy interest of the individual whose conversation is intercepted. The Supreme Court has made clear at least since *Katz v. United States*, 389 U.S. 347 (1967), that individuals have a substantial and constitutionally protected reasonable expectation of privacy that their telephone conversations will not be subject to governmental eavesdropping. The same privacy interest likely applies, absent individual circumstances lessening that interest, to the contents of e-mail communications. Although the individual privacy interests at stake may be substantial, it is well recognized that a variety of governmental interests – including routine law enforcement and foreign-intelligence gathering – can overcome those interests. (TS//SI-STLW//NF)

On the other side of the ledger here, the government’s interest in conducting the surveillance is the most compelling interest possible – securing the Nation from foreign attack in the midst of an armed conflict. One attack has already taken thousands of lives and placed the Nation in state of armed conflict. Defending the Nation from attack is perhaps the most

⁸⁵ Although this memorandum evaluates the STELLAR WIND program under the Fourth Amendment, we do not here analyze the specific procedures followed by the NSA in implementing the program. (TS//SI-STLW//NF)

~~TOP SECRET//COMINT-**[REDACTED]**STELLAR WIND**[REDACTED]**/NOFORN~~

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

important function of the federal government – and one of the few express obligations of the government enshrined in the Constitution. *See* U.S. Const. art. IV, § 4 (“The United States shall guarantee to every State in this Union a Republican Form of Government, *and shall protect each of them against Invasion . . .*”) (emphasis added). As the Supreme Court has declared, “[i]t is ‘obvious and unarguable’ that no governmental interest is more compelling than the security of the Nation.” *Haig v. Agee*, 453 U.S. 280, 307 (1981). *Cf. The Federalist* No. 23, at 148 (Alexander Hamilton) (Jacob E. Cooke ed. 1961) (“[T]here can be no limitation of that authority, which is to provide for the defence and protection of the community, in any matter essential to its efficacy.”). (TS//SI- STLW//NF)

As we have explained in previous memoranda, [REDACTED] the government’s overwhelming interest in detecting and thwarting further al Qaeda attacks is easily sufficient to make reasonable the intrusion into privacy involved in intercepting selected communications. The nation has already suffered one attack that disrupted the Nation’s financial center for days and that successfully struck at the command and control center for the Nation’s military. In initiating STELLAR WIND, moreover, the President specifically concluded that al Qaeda had the ability and intent to carry out further attacks that could result in massive loss of life and destruction of property and that might even threaten the continuity of the federal government. As noted above, the September 11 attack incorporated some aspects of a deliberate de-capitation strike aimed at the Nation’s capital. [REDACTED]

Of course, because the magnitude of the government’s interest here depends in part upon the threat posed by al Qaeda, it might be possible for the weight that interest carries in the balance to change over time. [REDACTED]

[REDACTED] It is thus significant for the reasonableness of the STELLAR WIND program that the President has established a system under which the surveillance is authorized only for a limited period, typically for 30 to 45 days. This ensures that the justification for the program is regularly reexamined. Indeed, each reauthorization is accompanied by a fresh reassessment of the current threat posed by al Qaeda. As explained above, before each reauthorization, the Director of Central Intelligence and the Secretary of Defense prepare a memorandum for the President highlighting some of the current information relating to threats from al Qaeda and providing their assessment as to whether al Qaeda still poses a substantial threat of carrying out an attack in the United States. Each Presidential Authorization of the program is thus based on a current threat assessment and includes the President’s specific determination that, based upon information available to him from all sources,

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

~~TOP SECRET//~~ [REDACTED] ~~/COMINT- STELLAR WIND~~ [REDACTED] ~~//NOFORN~~

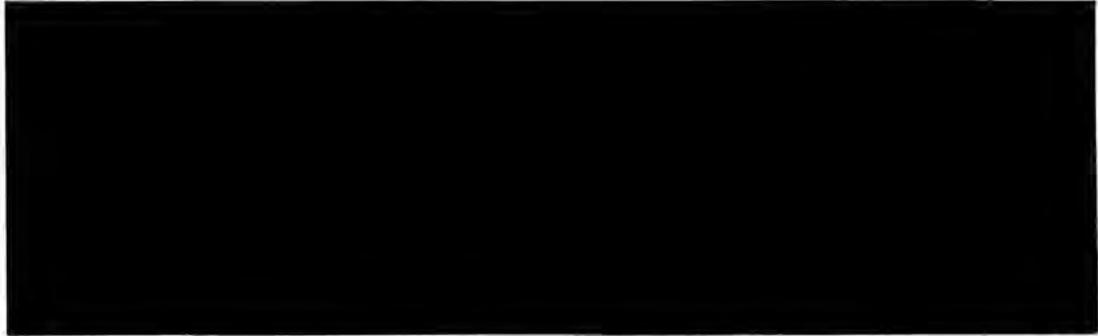


We should also note here [REDACTED] that, even based upon the limited range of information available to us – which is less than the totality of information upon which the President bases his decisions concerning the continuation of STELLAR WIND – there is ample basis on which to conclude that the threat posed by al Qaeda continues to be of a sufficient magnitude to justify the STELLAR WIND program for Fourth Amendment purposes. We note here only some of the highlights that have appeared in the threat-related intelligence reporting available to the President and relevant for evaluating the current threat posed by al Qaeda: (TS//SI-STLW//NF)

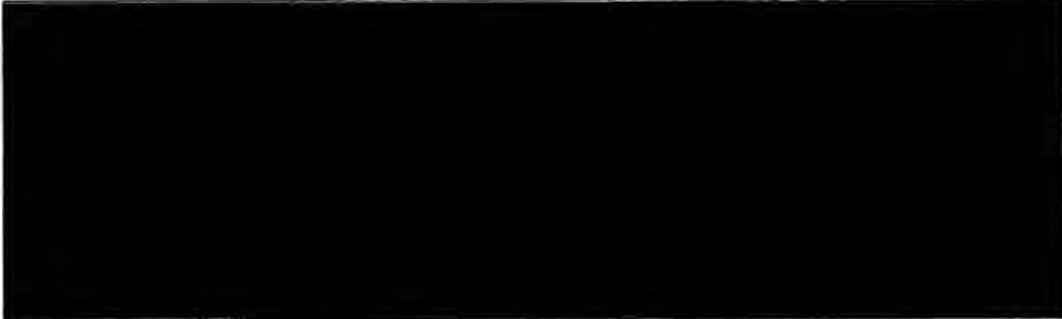
♦



♦

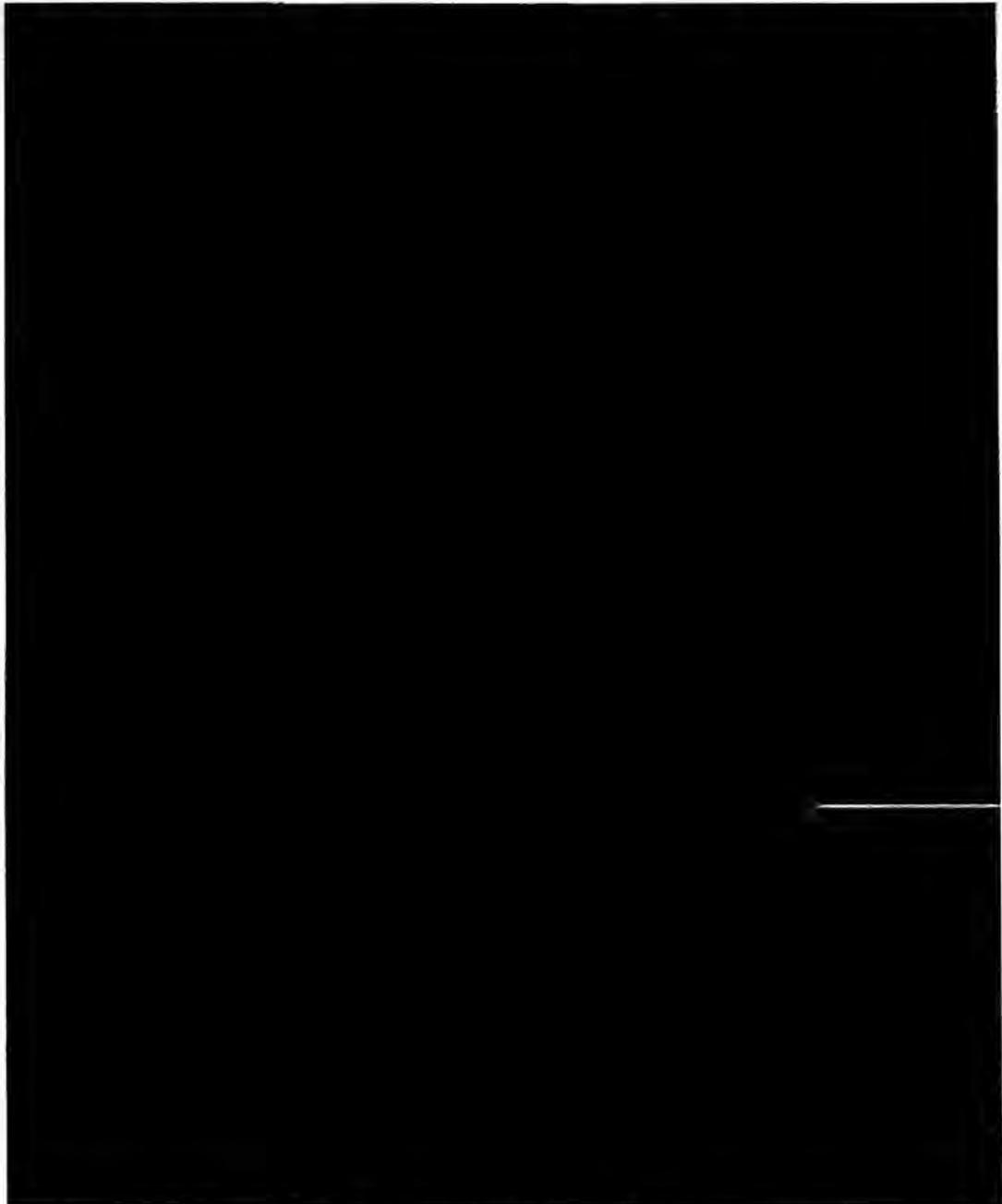


♦



~~TOP SECRET//~~ [REDACTED] ~~/COMINT- STELLAR WIND~~ [REDACTED] ~~//NOFORN~~

~~TOP SECRET// [REDACTED] //COMINT- STELLAR WIND [REDACTED] //NOFORN~~



Finally, as part of the balancing of interests to evaluate Fourth Amendment reasonableness, we think it is significant that content interception under STELLAR WIND is limited solely to those international communications for which "there are reasonable grounds to believe . . . [that] a party to such communication is a group engaged in international terrorism, or activities in preparation therefor, or any agent of such a group." March 11, 2004 Authorization [REDACTED] The interception is thus targeted precisely at communications for which there is already a reasonable basis to think there is a terrorism connection. This is relevant because (the Supreme

~~TOP SECRET// [REDACTED] //COMINT- STELLAR WIND [REDACTED] //NOFORN~~

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

Court has indicated that in evaluating reasonableness, one should consider the "efficacy of [the] means for addressing the problem." *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 663 (1995); *see also Earls*, 536 U.S. at 834 ("Finally, this Court must consider the nature and immediacy of the government's concerns and the efficacy of the Policy in meeting them."). This does not mean, of course, that reasonableness requires the "least intrusive" or most "narrowly tailored" means for obtaining information. To the contrary, the Supreme Court has repeatedly rejected such suggestions. *See, e.g., Earls*, 536 U.S. at 837 ("[T]his Court has repeatedly stated that reasonableness under the Fourth Amendment does not require employing the least intrusive means, because the logic of such elaborate less-restrictive-alternative arguments could raise insuperable barriers to the exercise of virtually all search-and-seizure powers.") (internal quotation marks omitted); *Vernonia*, 515 U.S. at 663 ("We have repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment."). Nevertheless, the Court has indicated that some consideration of the efficacy of the search being implemented – that is, some measure of fit between the search and the desired objective – is relevant to the reasonableness analysis.⁶⁶ Thus, a program of surveillance that operated by listening to the content of every telephone call in the United States in order to find those calls that might relate to terrorism would require us to consider a rather different balance here. STELLAR WIND, however, is precisely targeted to intercept solely those international communications for which there are reasonable grounds already to believe there is a terrorism connection, a limitation which further strongly supports the reasonableness of the searches.

(TS//SI-STLW//NF)

In light of the considerations outlined above, taking into account the totality of the circumstances, including the nature of the privacy interest at stake, the overwhelming governmental interest involved, the threat that al Qaeda continues to pose to the United States, and the targeted nature of the surveillance at issue, we conclude that the content interception undertaken through STELLAR WIND continues to be reasonable under the Fourth Amendment.

(TS//SI-STLW//NF)

⁶⁶ This consideration has often been relevant in cases that involve some form of suspicionless search. Even in those cases, moreover, the Court has made clear that the measure of efficacy required is not a stringent or demanding numerical measure of success. For example, in considering the use of warrantless road blocks to accomplish temporary seizures of automobiles to screen drivers for signs of drunken driving, the Court noted that the road blocks resulted in the arrest for drunken driving of only 1.6 percent of the drivers passing through the checkpoint. The Court concluded that this success rate established sufficient "efficacy" to sustain the constitutionality of the practice. *See Michigan Dep't of State Police v. Sitz*, 496 U.S. 444, 454-55 (1990). Similarly, the Court has approved the use of roadblocks that detected illegal immigrants in only 0.12 percent of the vehicles passing through the checkpoint. *See United States v. Martinez-Fuerte*, 428 U.S. 543, 554 (1976). What the Court has warned against is the use of random and standardless searches, giving potentially arbitrary discretion to officers conducting the searches, for which there is "no empirical evidence" to support the conclusion that they will promote the government objective at hand. *Sitz*, 496 U.S. at 454. (U)

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

~~TOP SECRET//COMINT--STELLAR WINE-/NOFORN~~

B. Acquisition of Meta Data Does Not Implicate the Fourth Amendment
(TS//SI-STLW//NF)

The Fourth Amendment analysis for the acquisition of meta data is substantially simpler. The Supreme Court has squarely determined that an individual has no Fourth Amendment protected "legitimate expectation of privacy regarding the numbers he dialed on his phone." *Smith v. Maryland*, 442 U.S. 735, 742 (1979) (internal quotation marks omitted). In *Smith*, the Court was considering the warrantless use of a pen register to record the numbers that a person had called on his telephone. In evaluating whether an individual could claim a reasonable expectation of privacy in such numbers, the Court explained that telephone subscribers know that they must convey the numbers they wish to call to the telephone company in order for the company to complete the call for them. In addition, subscribers know that the telephone company can and usually does record such numbers for billing purposes. As a result, the Court concluded that subscribers cannot claim "any general expectation that the numbers they dial will remain secret." *Id.* at 743. The situation fell squarely into the line of cases in which the Court had ruled that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743-44; *see also United States v. Miller*, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."). There could be, therefore, "no legitimate expectation of privacy here." 442 U.S. at 744.

First, e-mail users have no subjective expectation of privacy in e-mail meta data information. Just like the numbers that a caller dials on a telephone, the addressing information on an e-mail is freely shared with an e-mail service provider to enable the delivery of the

whether, for statutory purposes, the information is acquired through use of a "pen register" or instead through a request for business records is irrelevant for purposes of the constitutional analysis. The fact remains that the information gathered – the dialing number information showing with whom a person has been in contact – is not protected under the Fourth Amendment. (TS//SI-STLW//NF)

~~TOP SECRET//COMINT--STELLAR WINE-/NOFORN~~

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

message. The user fully knows that he must share that information to have his mail delivered.⁸⁸
(TS//SI-STLW//NF)

Second, even if a user could somehow claim a subjective expectation of privacy in e-mail meta data, that is not an expectation "that society is prepared to recognize as 'reasonable.'" *Katz*, 389 U.S. at 361 (Harlan, J., concurring). Just as telephone users who "voluntarily convey[]" information to the phone company "in the ordinary course" of making a call "assum[e] the risk" that this information will be passed on to the government or others, *Smith*, 442 U.S. at 744 (internal quotation marks omitted), so too do e-mail users assume the risk that the addressing information on their e-mails may be shared. Thus, such addressing information is simply not protected by the Fourth Amendment. (TS//SI-STLW//NF)

This conclusion is strongly supported by another analogy that could be used to assess the Fourth Amendment protection warranted for addressing information on e-mails - the analogy to regular letters in the U.S. mail. Lower courts have consistently concluded that the Fourth Amendment is not implicated by "mail covers," through which postal officials monitor and report for regular letter mail the same type of information contained in e-mail meta data - *i.e.*, information on the face of the envelope, including the name of the addressee, the postmark, the name and address of the sender (if it appears), and the class of mail. *See, e.g., United States v. Choate*, 576 F.2d 165, 174-77 (9th Cir. 1978); *cf. United States v. Charbonneau*, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997) ("E-mail is almost equivalent to sending a letter via the mails."); *United States v. Maxwell*, 45 M.J. 406, 418 (C.A.A.F. 1996) ("In a sense, e-mail is like a letter."). Courts have reasoned that "[s]enders knowingly expose[] the outsides of the mail to postal employees and others," *Choate*, 576 F.2d at 177, and therefore have "no reasonable expectation that such information will remain unobserved," *id.* at 175; *see also Vreeken v. Davis*, 718 F.2d 343, 347-48 (10th Cir. 1983) (concluding the "mail cover at issue in the instant case is indistinguishable in any important respect from the pen register at issue in *Smith*"); *United States v. DePoli*, 628 F.2d 779, 786 (2d Cir. 1980) ("[T]here is no reasonable expectation of privacy with regard to the outside of a letter . . ."); *United States v. Huie*, 593 F.2d 14, 15 (5th Cir. 1979) (*per curiam*) ("There is no reasonable expectation of privacy in information placed on the exterior of mailed items . . ."). Commentators have also recognized that e-mail addressing information is analogous to telephone numbers and mail covers, *see Orin S. Kerr, Internet Surveillance Law after the USA PATRIOT Act: The Big Brother That Isn't*, 97 Nw. U. L. Rev. 607, 611-15 (2003), and that, "[g]iven the logic of *Smith*, the [Supreme] Court is unlikely to recognize a constitutional difference between e-mail addressing information and the information that a telephone pen register reveals," Tracey Maclin, *Katz, Kyllo, and Technology*, 72 Miss. L.J. 51, 132 (2002). (TS//SI-STLW//NF)

⁸⁸ The *Smith* Court also noted that telephone customers must realize that telephone companies will track dialing information in some cases because it "aid[s] in the identification of persons making annoying or obscene calls." *Smith*, 442 U.S. at 742. The same subjective expectations hold true for users of Internet e-mail, who should know that ISPs can keep records to identify and suppress "annoying or obscene" messages from anonymous senders. Individuals are regularly bombarded with unsolicited, offensive material through Internet e-mail, and the senders of such e-mail intentionally cloak their identity. *See The CAN-SPAM Act of 2003*, Pub. L. No. 108-187, § 2(a), 117 Stat. 2699, 2699-700 (congressional findings on this point). (TS//SI-STLW//NF)

~~TOP SECRET//COMINT- STELLAR WIND//NOFORN~~

~~TOP SECRET~~ [REDACTED] ~~COMINT- STELLAR WIND~~ [REDACTED] ~~//NOFORN~~

In our view, therefore, well-established principles indicate that the collection of e-mail meta data does not qualify as a "search" implicating the Fourth Amendment.⁸⁹

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

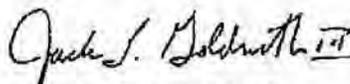
Thus, we affirm our conclusion that STELLAR WIND meta data collection does not involve the collection of information in which persons have a legitimate expectation of privacy and thus that it does not amount to a search under the Fourth Amendment. [REDACTED]

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

CONCLUSION (U)

For the foregoing reasons, we conclude that, notwithstanding the prohibitions of FISA and title 18, under the current circumstances of the ongoing armed conflict with al Qaeda and in light of the broad authority conferred in the Congressional Authorization, the President, as Commander in Chief and Chief Executive, has legal authority to authorize the NSA to conduct the signals-intelligence activities described above; that the activities, to the extent they are searches subject to the Fourth Amendment, comport with the requirements of the Fourth Amendment; and thus that the operation of the STELLAR WIND program as described above is lawful. ~~(TS//SI-STLW//NF)~~

Please let me know if we can be of further assistance. (U)



Jack L. Goldsmith, II
Assistant Attorney General

[REDACTED]

It should be clear from the discussion above that STELLAR WIND meta data collection involves the acquisition of data *both* for telephone calls *and* for e-mails and that our Fourth Amendment analysis above applies to both. ~~(TS//SI-STLW//NF)~~

~~TOP SECRET~~ [REDACTED] ~~COMINT- STELLAR WIND~~ [REDACTED] ~~//NOFORN~~

**First 22 pages of Document
Withheld in Full (b)(1), (b)(3)**

AUTHORITY FOR WARRANTLESS NATIONAL SECURITY SEARCHES

Presidents have long asserted the constitutional authority to order searches, even without judicial warrants, where necessary to protect the national security against foreign powers and their agents. The courts have repeatedly upheld the exercise of this authority.

A memorandum from President Franklin D. Roosevelt to Attorney General Robert H. Jackson, dated May 21, 1940, authorized the use of wiretaps in matters “involving the defense of the nation.” See *United States v. United States District Court for the Eastern District of Michigan*, 407 U.S. 297, 311 n.10 (1972) (“*Keith*”). The President directed the Attorney General “to secure information by listening devices [directed at] the conversation or other communications of persons suspected of subversive activities against the government of the United States, including suspected spies,” while asking the Attorney General “to limit these investigations so conducted to a minimum and to limit them insofar as possible as to aliens.” See *Electronic Surveillance Within the United States for Foreign Intelligence Purposes: Hearings Before the Subcomm. on Intelligence and the Rights of Americans of the Select Comm. on Intelligence, 94th Cong., 2d Sess. 24 (1976)* (statement of Attorney General Edward H. Levi) (“Levi Statement”). President Roosevelt issued the memorandum after the House of Representatives passed a joint resolution to sanction wiretapping by the FBI for national security purposes, but the Senate failed to act. See Americo R. Cinquegrana, *The Walls and Wires Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. Pa. L. Rev. 793, 797-98 (1989).

By a letter dated July 17, 1946, Attorney General Tom C. Clark reminded President Truman of the 1940 directive, which had been followed by Attorneys General Jackson and Francis Biddle. At Attorney General Clark’s request, the President approved the continuation of the authority, see Levi Statement at 24, and even broadened it to reach “internal security cases.” *Keith*, 407 U.S. at 311 and n.10. In the Eisenhower Administration, Attorney General Herbert Brownell, as the Supreme Court noted in *Keith*, advocated the use electronic surveillance both in internal and international security matters. 407 U.S. at 311.

In 1965, President Johnson announced a policy under which warrantless wiretaps would be limited to national security matters. Levi Statement at 26. Attorney General Katzenbach then wrote that he saw “no need to curtail any such activities in the national security field.” *Id.* Attorney General Richardson stated in 1973 that, to approve a warrantless surveillance, he would need to be convinced that it was necessary “(1) to protect the nation against actual or potential attack or other hostile acts of a foreign power, (2) to obtain foreign intelligence information deemed essential to the security of the United States, or (3) to protect national security information against foreign intelligence activities.” *Id.* at 27. When Attorney General Levi testified in 1976, he gave a similar list, adding that a warrantless surveillance could also be used “to obtain information certified as necessary for the conduct of foreign

affairs matters important to the national security of the United States.” *Id.*

Warrantless electronic surveillance of agents of foreign powers thus continued until the passage in 1978 of the Foreign Intelligence Surveillance Act, 18 U.S.C. §§ 1801-29. Although the Supreme Court never ruled on the legality of warrantless searches as to agents of foreign powers, *see Keith*, 407 U.S. at 321-22 (requiring a warrant in domestic security cases but reserving issue where a foreign power or its agents were involved), the courts of appeals repeatedly sustained the lawfulness of such searches. *United States v. Truong Dinh Hung*, 629 F.2d 908, 914 (4th Cir. 1980); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977); *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973); *United States v. Butenko*, 494 F.2d 593, 606 (3d Cir. 1974); *United States v. Clay*, 430 F.2d 165 (5th Cir. 1970), *rev'd on other grounds*, 403 U.S. 698 (1971); *but see Zweibon v. Mitchell*, 516 F.2d 594, 651 (D.C. Cir. 1975) (dictum in plurality opinion). The Fourth Circuit held, for example, that “because of the need of the executive branch for flexibility, its practical experience, and its constitutional competence, the courts should not require the executive to secure a warrant each time it conducts foreign intelligence surveillance.” *Truong*, 629 F.2d at 914. As the court elaborated, “attempts to counter foreign threats to the national security require the utmost stealth, speed, and secrecy,” and a “warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, in some cases delay executive response to foreign intelligence threats, and increase the chance of leaks regarding sensitive executive operations.” *Id.* at 913 (citations and footnote omitted). Furthermore, “the executive possesses unparalleled expertise to make the decisions whether to conduct foreign intelligence surveillance.” *Id.* (citations omitted). And “[p]erhaps most crucially, the executive branch not only has superior expertise in the area of foreign intelligence, it is also constitutionally designated as the pre-eminent authority in foreign affairs.” *Id.* at 914 (citations omitted). In this pre-statutory context, two courts of appeals, the Fourth Circuit in *Truong* (*id.* at 915) and the Third Circuit in *Butenko* (494 F.2d at 606), would have limited the authority to instances where the primary purpose of the search was to obtain foreign intelligence.”

The passage of FISA created an effective means for issuance of judicial orders for electronic surveillance in national security matters. Congress, however, had not given the Foreign Intelligence Surveillance Court the power to issue orders for physical searches. After nevertheless granting orders in three instances during the Carter Administration, the court ruled early in the Reagan Administration, as the Justice Department then argued, that it lacked jurisdiction to approve physical searches. *See S. Rep. 103-296*, at 36-37 (1994). Thus, physical searches after the ruling had to be approved by the Attorney General without a judicial warrant. *Id.* at 37. In 1994, after the use of warrantless physical searches in the Aldrich Ames case, Congress concluded that “from the standpoint of protecting the constitutional rights of Americans, from the standpoint of bringing greater legal certainty to this area, from the standpoint of avoiding problems with future espionage prosecutions, and from the standpoint of protecting federal officers and employees from potential civil liability,” *id.*, FISA should be amended to cover physical searches. *Id.* at 40.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER,)	
)	
Plaintiff,)	Civil No. 06-00096 (HHK)
)	
v.)	
)	
DEPARTMENT OF JUSTICE,)	
)	
Defendant.)	
<hr/>		
AMERICAN CIVIL LIBERTIES UNION, et al.,)	
)	Civil No. 06-00214 (HHK)
Plaintiffs,)	
)	
v.)	
)	
DEPARTMENT OF JUSTICE,)	
)	
Defendant.)	
<hr/>		

SECOND REDACTED DECLARATION OF STEVEN G. BRADBURY

I, Steven G. Bradbury, declare as follows:

- (U) I am the Principal Deputy Assistant Attorney General for the Office of Legal Counsel (“OLC” or the “Office”) of the United States Department of Justice (the “Department”). No one currently serves as the Assistant Attorney General for OLC. Consequently, in my capacity as Principal Deputy Assistant Attorney General for the Office, I am the head of OLC and supervise all OLC activities, including its responses to requests under the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552.
- (U) I provide this declaration in response to the Court’s Memorandum Opinion and Order of September 5, 2007 (“Mem. Op.”), requesting further information concerning the Department’s determination to withhold certain documents in response to

FOIA requests made by the Electronic Privacy Information Center (“EPIC”), the American Civil Liberties Union (“ACLU”), and the National Security Archive Fund (“NSAF”). Those FOIA requests sought information from OLC and other Department components regarding the Terrorist Surveillance Program (“TSP”), a classified foreign intelligence collection activity authorized by the President after the attacks of September 11, 2001.

3. (U) This declaration is based on my personal knowledge, information, and belief, and on information disclosed to me in my capacity as Principal Deputy Assistant Attorney General for OLC. This declaration also supplements, incorporates, and relies upon the In Camera, Ex Parte Declaration of Steven G. Bradbury, dated September 15, 2006 (cited herein as “Bradbury Decl.”), and also relies upon an exhibit to that Declaration, the In Camera, Ex Parte Declaration of John D. Negroponte, the former Director of National Intelligence, dated September 7, 2006 (cited herein as “DNI Decl.”).¹

4. (U) For the convenience of the Court, Exhibit A to this declaration is an updated version of the chart provided as Exhibit K to my original declaration, which lists each of the records or categories of records withheld by OLC in this litigation. The updated chart identifies, as to each record or category of record, whether summary judgment has been granted by the Court’s earlier order or whether the record is addressed in this supplemental submission, and if so, provides the paragraph numbers of this declaration where the record is discussed. In addition, in connection with the Notice of Supplemental Authority that I understand has been filed in this case advising the Court of developments in litigation in the United States District Court for the Southern District of New York – where certain documents processed by OLC in response to a similar FOIA request seeking information

¹ (U) In February 2007, J. Michael McConnell replaced Ambassador Negroponte as the Director of National Intelligence.

about the TSP have been at issue, and where I have also submitted a declaration – the chart attached hereto as Exhibit A also identifies those documents as to which summary judgment is still pending in the litigation before this Court but as to which OLC’s determinations to withhold have been upheld by the Court in The New York Times Company v. U.S. Dept. of Defense and U.S. Dept. of Justice, Civil Action No. 06-1553 (S.D.N.Y.) (Berman, J.).

(U) CLASSIFICATION OF DECLARATION

- 5. REDACTED
- 6. REDACTED
- 7. REDACTED
- 8. REDACTED
- 9. REDACTED

(U) PLAINTIFFS’ FOIA REQUESTS AND THE TERRORIST SURVEILLANCE PROGRAM

10. (U) Each of plaintiffs’ FOIA requests seeks information regarding the Terrorist Surveillance Program (“TSP”), a highly classified signals intelligence activity authorized by the President after the terrorist attacks on the United States of September 11, 2001. Under the TSP, the National Security Agency (“NSA”) was authorized to intercept the contents of international communications for which there were reasonable grounds to believe that one party was located outside the United States and that at least one party to the communication was a member or agent of al Qaeda or an affiliated terrorist organization. See Bradbury Decl. ¶ 19.

11. (U) The President publicly acknowledged the existence of the TSP on December 17, 2005. See Bradbury Decl. ¶ 20. On January 17, 2007, after my original declaration in this case was executed, the Attorney General announced that any electronic

surveillance that was occurring under the TSP would now be conducted subject to the approval of the Foreign Intelligence Surveillance Court (“FISC”). See Ex. B hereto. On August 5, 2007, Congress enacted the Protect America Act of 2007, Pub. L. No. 110-55, which exempted the acquisition of certain foreign intelligence information from the definition of “electronic surveillance” subject to the procedures of the Foreign Intelligence Surveillance Act (“FISA”). Under these circumstances, the President has not renewed his authorization of the TSP.

12. (U) Although the existence of the TSP is now publicly acknowledged, and some general facts about the TSP have been officially disclosed, the President has made clear that sensitive information about the nature, scope, operation, and effectiveness of the TSP and other communications intelligence activities remains classified and cannot be disclosed without causing exceptionally grave harm to U.S. national security. The declaration of the former Director of National Intelligence, provided in this litigation, sets forth the categories of information related to the TSP that cannot be disclosed without causing such harms, and describes these harms in detail. See DNI Decl. ¶¶ 22, 26-35.

13. REDACTED

14. REDACTED

15. REDACTED

16. REDACTED

(A.)

17. REDACTED

18. REDACTED

(B.)

19. REDACTED

20. REDACTED

21. REDACTED

22. REDACTED

(C.)

23. REDACTED

24. REDACTED

(U) FURTHER EXPLANATION OF WITHHOLDINGS

(U) A. Records or Categories of Records Relating to the President's Authorization of the TSP.

25. (U) Within this category, the Court has sought further justification concerning the proper withholding of the following documents: OLC 51, 63, 64, 114, and 115; ODAG 3 and 40; OIPR 138, 139, and 140; and FBI 4, 5, and 7, which are internal memoranda reflecting the views of Department officials regarding the President's reauthorization of the TSP and related matters. These documents reflect internal deliberations regarding the reauthorization process as well as the confidential advice of attorneys in the course of formulating recommendations to the President regarding these matters.

OLC 51

26. (U) OLC 51 is a one-page memorandum, dated August 9, 2004, from the Acting Assistant Attorney General for OLC to the Deputy Attorney General entitled "Proposed Memorandum," which contains OLC's advice concerning a decision to be made by the Deputy Attorney General regarding an intelligence collection activity.

27. REDACTED

Applicability of Exemption Five

28. (U) In any event, disclosure of OLC 51 would interfere with the attorney-client relationship between OLC and the leadership of the Department, which relies upon OLC for its legal advice with respect to a broad range of issues. Disclosure of communications of this nature would substantially harm the relationships intended to be protected by this privilege by compromising OLC's ability to provide legal advice and to do so in writing. Thus, OLC 51 is properly withheld under FOIA's Exemption Five.

OLC 63, OLC 64, OLC 114, OIPR 139, and OIPR 140

29. (U) OLC 63 is a two-page memorandum (and related electronic file) dated March 16, 2004, from the Acting Attorney General to the Counsel to the President, copied to the President's Chief of Staff, containing legal recommendations regarding classified foreign intelligence activities. OLC 63 is withheld under FOIA Exemptions One, Three, and Five.

30. (U) OLC 64 consists of four copies of a three-page memorandum dated March 15, 2004, for the Deputy Attorney General from the Assistant Attorney General for OLC, plus an electronic file, which outlines preliminary OLC views with respect to certain legal issues concerning classified foreign intelligence activities. The memorandum specifically notes that OLC's views have "not yet reached final conclusions" and that OLC is "not yet prepared to issue a final opinion." OLC 64 is withheld under FOIA Exemptions One, Three, and Five.

31. (U) OLC 114 consists of two copies of a three-page memorandum dated March 22, 2004, to the Deputy Attorney General from the Assistant Attorney General for OLC, which confirms oral advice provided by OLC on a particular matter concerning classified foreign intelligence activities. OLC 114 is withheld under FOIA Exemptions One, Three, and Five.

32. (U) OIPR 139 is a one-page memorandum dated March 12, 2004, to the Deputy Attorney General from the Assistant Attorney General for OLC, which provides legal advice concerning certain decisions relating to classified foreign intelligence activities. OIPR 139 is withheld under FOIA Exemptions One, Three, and Five.

33. (U) OIPR 140 is a one-page letter dated March 11, 2004, from the Assistant Attorney General for OLC, to the White House Counsel seeking clarification regarding advice that OLC had been requested to provide concerning classified foreign intelligence activities. OIPR 140 is withheld under FOIA Exemptions One, Three, and Five.

Applicability of Exemptions One and Three.

34. REDACTED

35. REDACTED

Applicability of Exemption Five.

36. (U) Disclosure of each of these documents would interfere with privileged attorney-client relationships. Specifically, disclosure of OLC 64, OLC 114, and OIPR 139, which contain recommendations and legal advice from OLC to the Deputy Attorney General, would interfere with the attorney-client relationship between OLC and Department leadership who rely upon OLC for its legal advice with respect to a broad range of issues. Disclosure of communications of this nature would substantially harm the relationships intended to be protected by the attorney-client privilege by compromising OLC's ability to provide legal advice and to do so in writing. Thus, OLC 64, OLC 114, and OIPR 139 are properly withheld under FOIA's Exemption Five.

37. (U) Similarly, disclosure of OLC 63, which contains recommendations and legal advice from the Department to the President and his advisors, would interfere with the attorney-client relationship between the Department of Justice and White House officials,

who rely upon the Department for its legal advice with respect to a broad range of issues. Disclosure of communications of this nature would substantially harm the relationships intended to be protected by the attorney-client privilege by compromising the Department's ability to provide candid legal advice and to do so in writing. Thus, OLC 63 is also properly withheld under Exemption Five.

38. (U) OIPR 140 is similarly exempt from disclosure in that it is a protected attorney-client communication between OLC and the White House seeking clarification regarding a question put to OLC with respect to a particular request for legal advice that was then pending in OLC. Disclosure of this sort of document would demonstrate the nature of the advice sought from OLC, and the nature of the clarification request that OLC then made of the White House, each of which are confidential communications that are protected by the attorney-client privilege. OIPR 140, accordingly, is properly withheld in its entirety under FOIA Exemption Five.

39. (U) In addition, all of these documents (and particularly OLC 64, which notes, on its face, that OLC's views have "not yet reached final conclusions" and that OLC is "not yet prepared to issue a final opinion") were part of an ongoing decisionmaking process, whereby certain advice and recommendations were provided by OLC and the Department in the course of decisions by the President concerning the continued authorization of particular foreign intelligence activities. Disclosure of predecisional, deliberative documents that were part of ongoing decisionmaking would seriously undermine the process by which the Government makes decisions by discouraging the frank exchange of ideas critical to effective decisionmaking. Thus, OLC 63, OLC 64, OLC 114, OIPR 130, and OIPR 140 are also properly withheld under the deliberative process privilege component of Exemption Five.

OLC 115

40. (U) OLC 115 is a two-page memorandum for the Attorney General from a Deputy Assistant Attorney General, OLC, dated January 9, 2002, which relates to the Attorney General's review of the legality of the President's order authorizing the TSP in the course of considering that program's reauthorization, which was done approximately every 45 days. See Bradbury Decl. ¶ 30. OLC 115 is withheld under FOIA Exemptions One, Three, and Five.

(U) *Applicability of Exemptions One & Three.*

41. REDACTED

(U) *Applicability of Exemption Five.*

42. (U) In addition, as discussed in my earlier declaration, OLC 115 reflects internal deliberations regarding the process by which the TSP was authorized. See Bradbury Decl. ¶ 40. This document contains a recommendation from OLC to the Attorney General concerning his review of the legality of the TSP in the course of its periodic reauthorization. To disclose such deliberative recommendations from OLC to the Attorney General would compromise the process by which the Attorney General receives advice from OLC attorneys, see id. ¶ 5, and would disclose the factors and recommendations presented to the Attorney General for his consideration when making certain decisions concerning the TSP. Both the deliberative process privilege and the attorney-client privilege are intended to protect against compromising the confidentiality of these types of communications, and, accordingly, OLC 115 is also properly withheld under Exemption Five.

ODAG 3

43. (U) ODAG 3 is a duplicate of OLC 115 and is withheld for the reasons explained in paragraphs 40-42, supra.

ODAG 40

44. (U) ODAG 40 is a one-page undated document (plus an electronic file) which contains the personal notes of a former Department attorney concerning matters relating to classified foreign intelligence activities. This document is withheld under FOIA Exemptions One, Three, and Five.

(U) Applicability of Exemptions One & Three.

45. **REDACTED**

(U) Applicability of Exemption Five.

46. (U) As described in my prior declaration, ODAG 40 reflects internal deliberations regarding the process of reauthorizing the TSP, as well as the confidential advice of attorneys in the course of formulating recommendations to the President regarding classified communications intelligence activities. See Bradbury Decl. ¶ 39. The substance of the communications contained in these notes is protected under a variety of privileges. For example, the notes reflect communications between OLC and a senior adviser to the President related to presidential decisionmaking concerning intelligence collection activities, and thus, are protected by the presidential communications privilege. The notes also reflect the substance of communications related to advice from OLC to the NSA that is protected by the attorney-client privilege, as well as internal Executive Branch deliberations within the Department, and involving other agencies, that are protected by the deliberative process privilege. Disclosure of communications of this nature would substantially harm the relationships and confidentiality concerns intended to be protected by these privileges, and, thus, ODAG 40 is properly withheld under FOIA's Exemption Five.

47. **REDACTED**

OIPR 138

48. (U) In reviewing OIPR 138 for purposes of preparing this declaration, I have observed that the document is subject to an express reservation of control by the White House. As with OLC 56, 57, and 58, which OLC previously determined did not constitute agency records as that term is defined in FOIA, see Bradbury Decl. ¶ 77, OLC has no authority to distribute this record or to dispose of it. OIPR 138, accordingly, is not an “agency record,” as that term is defined in FOIA, and should not have been processed by OLC in response to the three FOIA requests at issue in this litigation. Because plaintiffs do not challenge OLC’s determinations with respect to records that are not Department of Justice records, this record is not further discussed herein.

FBI 4

49. (U) FBI 4 is a duplicate of OLC 63 and is withheld for the reasons explained in paragraphs 29, 34-35, 37, 39, supra.

FBI 5

50. (U) FBI 5 is a duplicate of OLC 64 and is withheld for the reasons explained in paragraphs 30, 34-36, 39, supra.

FBI 7

51. (U) FBI 7 is a one-page memorandum, dated October 20, 2001, from the Attorney General to the Director of the FBI, advising the Director that certain intelligence collection activities are legal and have been appropriately authorized. The memorandum is classified TOP SECRET and is withheld under FOIA Exemptions One and Three.

52. **REDACTED**

REMAINING DOCUMENTS IN CATEGORY A

53. (U) The Court has upheld OLC's withholding of the remaining records contained within this category, identified and described in my previous declaration at paragraphs 32-38: OLC 34, 67, 74, 78, 93, and 101; ODAG 10, 17, 18, 19, 48, and 65; and OIPR 141. See Mem. Op. at 14.

B. REDACTED

54. (U) The documents withheld by OLC in Category B related to certain arrangements and activities necessary to the operation of the foreign intelligence activities authorized by the President. Further information about this category of documents cannot be provided without disclosing classified information.

55. **REDACTED**

56. (U) The Court has upheld OLC's withholding of all the records contained within this category, identified and described in my previous declaration at paragraphs 42-47: OLC 35, 36, 37, 75 and 207, and ODAG 12.

C. (U) Records or Categories of Records Relating to Targets of the TSP.

57. (U) Within this category, the Court has sought further justification regarding the proper withholding of the following documents: OLC 76, 107, 139, 144, 145, and 200, ODAG 15, 16, 23 and 24, and OIPR 9.

OLC 76 and ODAG 24

58. (U) As described in my earlier declaration, see Bradbury Decl. ¶ 48, OLC has been part of an extensive interagency process designed to identify organizations affiliated with al Qaeda for purposes of the surveillance authorized under the TSP and to develop the criteria to be applied when identifying potential targets. OLC thus withheld records or

categories of records relating to the criteria used for targeting and the appropriateness of targeting certain groups or individuals under the TSP.

59. (U) These interagency discussions were intended to ensure that the TSP operated in a manner consistent with the President's authorizations and were part of the Department's review of the President's authorizations for form and legality. In addition, much of this interagency discussion occurred in the course of the Department's extended effort to devise an application for the FISC that would, if granted, allow activities authorized by the President under the TSP to be placed under FISC authorization. This extended effort required consultation among a variety of intelligence agencies and components to ensure that the application made to the FISC sought authorization for a surveillance effort that was appropriately targeted to ensure that useful information could be obtained through intelligence collection efforts and in compliance with applicable legal requirements.

60. (U) OLC 76 and ODAG 24 are categories of records that reflect this interagency discussion. The documents are identified in a log attached hereto as Exhibit C. As that log demonstrates, the documents withheld by OLC in this category of records fall into three overlapping categories: interagency communications, much of it preliminary, concerning consideration of international terrorist groups potentially affiliated with al Qaeda; OLC drafts and notes concerning the same, often identifying questions requiring interagency resolution; and intelligence information and analysis concerning terrorist groups considered relevant to such consideration. All of these documents are properly withheld under FOIA Exemptions One, Three, and Five.

Applicability of Exemptions One and Three.

61. (U) As described in my prior declaration, the United States cannot confirm or deny the identities of any target of foreign surveillance without fundamentally compromising

the intelligence sources and methods as well as intelligence information that might be collected from that source. See Bradbury Decl. ¶ 50; DNI Decl. ¶ 35. To disclose any of the discussion contained in these documents, preliminary or otherwise, concerning consideration of international terrorist groups potentially affiliated with al Qaeda, and whose members or agents, accordingly, might be targeted for collection under the TSP, would identify the priorities of United States intelligence collection activities, and put persons affiliated with these groups on notice that their communications may be compromised, inevitably resulting in the loss of intelligence information. See Bradbury Decl. ¶¶ 51-52; DNI Decl. ¶ 35.

62. **REDACTED**

Applicability of Exemption Five

63. (U) As described in my earlier declaration, all of the documents identified in this section were created or collected as part of an ongoing interagency deliberative process concerning consideration of groups potentially affiliated with al Qaeda. Moreover, although factual information is ordinarily not subject to deliberative process protection, in this case the selection of the specific facts considered by the Department and other agencies involved in this process would reveal the nature of the process and the specific information recommended to be considered when identifying groups potentially affiliated with al Qaeda. Disclosure of these records or categories of records would compromise the interagency deliberative process and deter the full exchange of ideas and information intended to assist in that process, to the detriment of informed government decisionmaking. Such documents are protected by the deliberative process privilege, and thus are properly withheld under FOIA's Exemption Five.

64. (U) Furthermore, many of the documents withheld in this category constitute attorney-client communications between OLC and other Department attorneys, and the other

agencies, particularly in the Intelligence Community, to which we provide legal advice. To disclose these communications would hamper that relationship and make it difficult for the Department to request and for the client agencies to provide factual information and opinions critical to producing well-informed legal opinions from the Department that can support effective decisionmaking at the agency level. Documents reflecting these attorney-client communications, accordingly, are properly withheld under FOIA's Exemption Five.

65. (U) In addition, deliberations concerning the nature and scope of an application for a FISC order relating to interception of the content of one-end foreign communications were ongoing at the time the plaintiffs' FOIA requests were processed in the spring of 2006. Because these deliberations occurred in the context of preparing for a court filing, and involved views submitted at the request of the OLC attorneys that were preparing the filing, all of these documents are protected by the attorney work product doctrine, and, thus, are properly withheld in their entirety.

OLC 107

66. (U) OLC 107 consists of four copies of a two-page document that addresses generally standards for considering whether international terrorist groups would be considered to be potentially affiliated with al Qaeda. This document is identified on its face as "preliminary" and thus constitutes a draft. It is my understanding that plaintiffs do not contest OLC's determination to withhold drafts, and thus OLC 107 is not discussed further herein.²

² (U) All of the draft documents withheld by OLC are withheld under Exemption Five, but most are also properly withheld under other exemptions, including under Exemptions One and Three. Because plaintiffs concede that these draft documents are properly withheld under Exemption Five, other equally applicable and overlapping exemptions are not further discussed.

OLC 139

67. (U) OLC 139 consists of three copies of a six-page document, all with handwritten comments and marginalia, entitled “Factors.” This document is a draft of a portion of a proposed submission to the FISC concerning the factors to be considered in decisions regarding targeting, and is withheld under FOIA Exemptions One, Three, and Five. It is my understanding that plaintiffs do not contest OLC’s determination to withhold drafts, and thus OLC 139 is not discussed further herein.

OLC 144

68. (U) OLC 144 consists of five copies of a two-page draft memorandum setting forth preliminary views on standards for considering whether international terrorist groups might be considered to be potentially affiliated with al Qaeda, with handwritten comments and marginalia. It is my understanding that plaintiffs do not contest OLC’s determination to withhold drafts, and thus OLC 144 is not discussed further herein.

OLC 145 and ODAG 15

69. (U) OLC 145 and ODAG 15 are copies of two different classified intelligence reports provided to the Department by an intelligence agency in connection with, and for the purpose of, the preparation of legal advice. These reports also contain classified information that may have been collected through the use of classified intelligence sources and methods. As explained in my prior declaration, the Department has conferred with the intelligence agencies that provided or compiled this information and has been advised that the disclosure of such sensitive intelligence information would both endanger the sources and methods through which it was obtained and also compromise the capabilities of the United States Intelligence Community to continue to secure such intelligence information in the future. See also DNI Decl. ¶ 26. They advise that such a result would have an exceptionally grave

effect on U.S. national security. This material, accordingly, is properly and currently classified, and is exempt from disclosure under FOIA Exemptions One and Three.³

OLC 200

70. (U) OLC 200 is a typewritten note, with attachments, totaling 11 pages, plus a related electronic file, from one of my staff attorneys to me which discusses a legal question relating to foreign intelligence activities. This document is withheld under FOIA Exemptions One, Three and Five.

Applicability of Exemptions One & Three.

71. (U) The legal analysis contained in this document was derived from, and summarizes, a classified NSA operational directive that was provided to OLC in the course of performing its function of providing advice to other Executive Branch agencies. Because the NSA directive remains classified, this derivative document cannot be disclosed without compromising the national security information contained in that document. Accordingly, it is properly withheld under Exemptions One and Three.

Applicability of Exemption Five.

72. (U) Disclosure of such intra-OLC communications conveying information from staff level attorneys to their supervisors would fundamentally undermine the manner in which this office conducts business. I rely upon my staff to provide me with concise legal explanations and analysis on topics of interest, and it is not unusual that they are asked to do so in writing. To require the disclosure of such informal communications when they are reduced to writing would seriously impinge on my ability – and the ability of my staff – to fulfill our duties to the Department.

³ (U) Although certain portions of these intelligence reports are marked as unclassified, those sections do not address the TSP, and thus the unclassified portions of these reports are not responsive to the plaintiffs' FOIA requests and are not required to be disclosed.

ODAG 16

73. (U) ODAG 16 is a duplicate of OLC 145 and is withheld for the reasons explained in paragraph 69, supra.

ODAG 23

74. (U) ODAG 23 is a six-page memorandum, dated August 18, 2005, from an intelligence agency official to OLC attorneys discussing classified intelligence concerning consideration of international terrorist groups potentially affiliated with al-Qaeda. This document is part of the interagency discussion described above at paragraphs 58-60, and is withheld under FOIA Exemptions One, Three, and Five for all of the reasons stated therein.

OIPR 9

75. (U) OIPR 9 is a copy of an undated three-page memorandum from an intelligence agency official to another intelligence agency official concerning consideration of particular international terrorist groups potentially affiliated with al Qaeda. This document is part of the interagency discussion described above at paragraphs 58-60, and is withheld under FOIA Exemptions One, Three, and Five for all of the reasons stated therein.

REMAINING DOCUMENTS IN CATEGORY C

76. (U) Several of the documents contained within this category also fell within Category A, and their withholding was upheld by the Court in connection with its decisions regarding that category. Specifically, the Court has upheld OLC's withholding of the following records, identified and described in my previous declaration at paragraphs 32-33 and 49: OLC 78 and ODAG 10, 17, 18, and 19. See Mem. Op. at 14.

D. (U) Records or Categories of Records Relating to Matters Before the Foreign Intelligence Surveillance Court.

77. (U) The Court has upheld OLC's withholding of all the records contained within this category, see Mem. Op. at 15, which consisted of documents associated with the drafting of applications or other pleadings filed with the FISC, and correspondence with that Court.

78. (U) The documents as to which OLC has been granted summary judgment contained within this category were identified and described in my previous declaration at paragraphs 54-59: OLC 1, 2, 3, 4, 5, 6, 10, 11, 15, 18, 19, 22, 23, 55, 66, 68, 69, 72, 73, 92, 100, 104, 109, 110, 111, 112, 122, 124, 130, 136, and 137; ODAG 7, 26, 28, 30, 33 and 58; and OIPR 25, 27, 71, and 94. See Mem. Op. at 15.

E. (U) Records or Categories of Records Relating to Legal Opinions of OLC.

79. (U) Within this category, the Court has sought further justification regarding the proper withholding of the following documents: OLC 16, 54, 59, 62, 85, 113, 129, 131, 132, 133, 146, and 201; ODAG 1, 2, 5, 6, 38, 42, and 52; OIPR 28, 29, 37, and 60; and FBI 42 and 51.

80. (U) Before discussing these particular documents, it is important to address the unique function of OLC and the unique expectations associated with legal memoranda generated by OLC. The principal function of OLC is to assist the Attorney General in his role as legal adviser to the President and to other departments and agencies in the Executive Branch. In connection with this function, OLC prepares memoranda addressing a wide range of legal questions involving operations of the Executive Branch, and participates in assisting in the preparation of legal documents and providing more informal legal advice as necessary and requested. A significant portion of OLC's work can be divided into two categories.

First, OLC renders opinions that resolve disputes within the Executive Branch on legal questions. Second, OLC performs a purely advisory role as legal counsel to the Attorney General, providing confidential legal advice both directly to the Attorney General, and through him or on his behalf, to the White House and other components of the Executive Branch.

81. (U) Although OLC's legal advice and analysis may inform decisionmaking on policy matters, the legal advice is not itself dispositive as to any policy adopted by the Executive Branch. OLC does not purport, and in fact lacks authority, to make any policy decisions. OLC's role is to advise, not to mandate that its advice be implemented into agency policy. Although on some occasions, specific OLC memoranda have been drafted with the expectation that they will be made public, and although some OLC documents are ultimately selected for publication, generally OLC memoranda are prepared with the expectation that they will be held in confidence, and that is of course the case with classified OLC opinions and related documents.

OLC 16, 54, 59, 62, 85, 129, 131, 132, and 146

82. (U) These nine documents are OLC memoranda prepared in response to particular requests for OLC advice either from within the Department or from elsewhere within the Executive Branch in the context of decisions being made regarding the legal parameters of foreign intelligence activities in the months and years following the terrorist attacks of September 11, 2001. Each of these memoranda was prepared in OLC's advisory capacity and with the expectation that the legal advice provided by OLC was to be held in confidence. Although, as described above, OLC advice often informs Administration decisionmaking, none of these advisory memoranda announced or established Administration

policy, but rather provided advice, analysis, and/or recommendations in response to requests for OLC views.

83. (U) The nine final memoranda withheld by OLC are:
- a. (U) OLC 16, which consists of four copies, one with handwritten marginalia, of a 12-page memorandum, dated February 25, 2003, for the Attorney General from a Deputy Assistant Attorney General for OLC, prepared in response to a request from the Attorney General for legal advice concerning the potential use of certain information collected in the course of classified foreign intelligence activities. OLC 16 is withheld under FOIA Exemptions One, Three, and Five.
 - b. (U) OLC 54, which consists of six copies, some with handwritten comments and marginalia, of a 108-page memorandum, dated May 6, 2004, from the Assistant Attorney General for OLC to the Attorney General, as well as four electronic files, one with highlighting, prepared in response to a request from the Attorney General that OLC perform a legal review of classified foreign intelligence activities. OLC 54 is withheld under FOIA Exemptions One, Three, and Five.
 - c. (U) OLC 59, which consists of four copies of an 18-page memorandum for the file, dated November 17, 2004, from the Acting Assistant Attorney General in OLC, plus an electronic file, prepared in response to a request for OLC views regarding the applicability of certain statutory requirements. OLC 59 is withheld under FOIA Exemptions One, Three, and Five.
 - d. (U) OLC 62, which consists of two copies, one with highlighting and marginalia by an OLC attorney, of a February 8, 2002, memorandum from a Deputy Assistant Attorney General in OLC to the General Counsel of another federal agency,

prepared in response to a request for OLC views regarding the legality of certain hypothetical activities. OLC 62 is withheld under FOIA Exemptions One, Three, and Five.

e. (U) OLC 85, which is a nine-page memorandum, with highlighting, dated July 16, 2004, from the Assistant Attorney General in OLC to the Attorney General, evaluating the implications of a recent Supreme Court decision for certain foreign intelligence activities. OLC 85 is withheld under FOIA Exemptions One, Three, and Five.

f. (U) OLC 129, which consists of two copies, one with handwritten comments and marginalia, of a nine-page memorandum, dated October 11, 2002, from a Deputy Assistant Attorney General in OLC to the Attorney General, prepared in response to a request for OLC's views concerning the legality of certain communications intelligence activities. OLC 129 is withheld under FOIA Exemptions One, Three, and Five.

g. (U) OLC 131, which consists of two copies, both with underscoring and marginalia, of a 24-page memorandum, dated November 2, 2001, from a Deputy Assistant Attorney General in OLC to the Attorney General, prepared in response to a request from the Attorney General for OLC's opinion concerning the legality of certain communications intelligence activities. OLC 131 is withheld under FOIA Exemptions One, Three, and Five.

h. (U) OLC 132, which consists of two copies, one with handwritten comments and marginalia, of a 36-page memorandum, dated October 4, 2001, from a Deputy Assistant Attorney General in OLC to the Counsel to the President, created in response to a request from the White House for OLC's views regarding what legal standards might govern the use of certain intelligence methods to monitor communications by potential terrorists. OLC 132 is withheld under FOIA Exemptions One, Three, and Five.

i. (U) OLC 146, which is a 37-page memorandum, dated October 23, 2001, from a Deputy Assistant Attorney General in OLC, and a Special Counsel, OLC, to the Counsel to the President, prepared in response to a request from the White House for OLC's views concerning the legality of potential responses to terrorist activity. OLC 146 is withheld under FOIA Exemption Five.

Applicability of Exemptions One and Three.

84. REDACTED

Applicability of Exemption Five.

85. (U) The nine documents identified above were all prepared by OLC in its role of assisting the Attorney General in the discharge of his responsibilities as legal adviser to the President and heads of the Executive Branch departments and agencies. In preparing these documents, OLC was performing a purely advisory role, providing legal advice and assistance. Thus, the nine final memoranda withheld by OLC in this category were created in response to specific requests for OLC advice on particular topics. OLC's preparation and provision of advice to the White House and other Executive Branch agencies is part of the process of attorney-client communications that would be seriously disrupted if such documents are publicly disclosed. As described in my prior declaration, the White House and other Executive Branch agencies rely upon OLC to provide candid and useful advice on a range of issues, including difficult and complex legal questions critical to national security. See Bradbury Decl. ¶ 63-64. To disclose such communications between OLC attorneys and our clients would fundamentally disrupt the attorney-client relationship and would deter federal agencies and officials in the White House from seeking timely and appropriate legal advice. Id.

86. (U) Compelled disclosure of these advisory and pre-decisional documents would cause substantial harm to the deliberative process of the Department of Justice and the Executive Branch and disrupt the attorney-client relationship between the Department and the President and other officers of the Executive Branch. Attorneys in OLC are often asked to provide advice and analysis with respect to very difficult and unsettled issues of law. Frequently, such issues arise in connection with highly complex and sensitive operations of the Executive Branch. It is essential to the mission of the Executive Branch that OLC legal advice, and the development of that advice, not be inhibited by concerns about public disclosure. Protecting the confidentiality of documents that contain such advice is essential in order to ensure both that creative and even controversial legal arguments and theories may be explored candidly, effectively, and in writing, and to ensure that Executive Branch officials will continue to request legal advice from OLC on such sensitive matters.

87. (U) Particularly in light of the Nation's ongoing fight against global terrorism, and the public interest in the effective performance of these activities, the need of the President and the heads of Executive Branch departments and agencies for candid, thoroughly considered legal advice when considering potential executive actions is especially compelling. Thus, all nine of the documents identified in paragraph 83, supra, constitute documents subject to the deliberative process and attorney-client communication privileges, and moreover, those provided to inform a decision to be made by the President are also subject to the presidential communications privilege. As such, all of these documents are properly withheld as exempt in their entirety under FOIA Exemption Five.

88. (U) I have specifically reviewed each of the documents identified in paragraph 83 and have determined that all portions of these documents contain either classified information or deliberative and privileged legal advice and analysis of OLC.

89. (U) In assessing the determination stated in paragraph 88, it is useful to recall that, with respect to the TSP in particular, the Department of Justice publicly released an extensive legal analysis of the TSP shortly after its existence was acknowledged by the President in December 2005. The Department's January 19, 2006, "White Paper," which is available at www.usdoj.gov, and was released to the plaintiffs in this litigation, provides the official view of the Department with respect to the legality of the TSP from which classified and privileged information has already been removed for public disclosure.

OLC 113

90. (U) OLC 113 consists of three copies of a one-page memorandum, dated September 15, 2004, from the Deputy Attorney General to the Director of the Federal Bureau of Investigation, entitled "National Security Agency Collection Activity." This document is withheld under FOIA Exemptions One and Three.

91. **REDACTED**

OLC 133

92. OLC 133 is a duplicate of ODAG 51, as to which I understand the Court has already granted summary judgment, and which was responsive only for certain handwritten notes that appeared on the copy of the document maintained in ODAG. See Mem. Op. at 16; Bradbury Decl. ¶ 66 n. 8. Accordingly, this document is not further discussed herein.

ODAG 1

93. (U) ODAG 1 is a duplicate of OLC 54, as well as of OIPR 28, and is withheld for the reasons explained in paragraphs 82-89, supra.

ODAG 2

94. (U) ODAG 2 consists of three additional copies, two with underscoring and marginalia by a Department attorney, of the memorandum described as OLC 131, as well as OIPR 37 and FBI 51, and is withheld for the reasons explained in paragraphs 82-89, supra.

ODAG 5

95. (U) ODAG 5 is a duplicate of OLC 132 and is withheld for the reasons explained in paragraphs 82-89, supra.

ODAG 6

96. (U) ODAG 6 is a duplicate of OLC 129 and is withheld for the reasons explained in paragraphs 82-89, supra.

ODAG 38

97. (U) ODAG 38 is a duplicate of OLC 16 and is withheld for the reasons explained in paragraphs 82-89, supra.

ODAG 42

98. (U) ODAG 42 is a 19-page memorandum, dated May 30, 2003, from a Deputy Assistant Attorney General in OLC to the General Counsel of another Executive Branch agency. This document is withheld under FOIA Exemptions One, Three, and Five.

(U) Applicability of Exemptions One & Three.

99. REDACTED

100. REDACTED

(U) Applicability of Exemption Five.

101. (U) OLC's preparation and provision of advice to other Executive Branch agencies is part of the process of attorney-client communications that would be seriously disrupted if such documents, whether in draft or final form, are publicly disclosed. As

described in my prior declaration, Executive Branch agencies rely upon OLC to provide candid and useful advice on a range of issues, including difficult and complex legal questions critical to national security. See Bradbury Decl. ¶¶ 63-64. To disclose such communications between OLC attorneys and our federal agency clients would fundamentally disrupt the attorney-client relationship and would deter federal agencies from seeking timely and appropriate legal advice. See id. Thus, for this reason as well, ODAG 42, which is a memorandum prepared at the request of another Executive Branch agency, is properly withheld under FOIA's Exemption Five.

ODAG 52

102. (U) ODAG 52 is a duplicate of OLC 62 and is withheld for the reasons explained in paragraphs 82-89, supra.

OIPR 28

103. (U) OIPR 28 is a duplicate of OLC 54, as well as of ODAG 1, and is withheld for the reasons explained in paragraphs 82-89, supra.

OIPR 29

104. (U) OIPR 29 is a duplicate of OLC 59 and is withheld for the reasons explained in paragraphs 82-89, supra.

OIPR 37

105. (U) OIPR 37 is a duplicate of OLC 131, as well as of ODAG 2 and FBI 51, and is withheld for the reasons explained in paragraphs 82-89, supra.

FBI 42

106. (U) FBI 42 is a duplicate of OLC 113 and is withheld for the reasons explained in paragraphs 90-91, supra.

FBI 51

107. (U) FBI 51 is a duplicate of OLC 131, as well as of ODAG 2 and OIPR 37, and is withheld for the reasons explained in paragraphs 82-89, supra.

REMAINING DOCUMENTS IN CATEGORY E

108. (U) The Court has upheld OLC's withholding of the remaining documents in this category, identified and described in my previous declaration at paragraphs 66-70: OLC 8, 9, 26, 27, 28, 29, 32, 40, 41, 42, 43, 53, 60, 61, 71, 77, 79, 83, 86, 87, 88, 89, 94, 102, 103, 106, 108, 118, 119, 120, 121, 123, 140, 141, 142, 143, 203, 204, 205, 206, and 208; ODAG 8, 21, 22, 43, 44, 45, 49, 50, 51, and 53; and OIPR 1, 2, 32, 33, 34, 35, 75 and 129, and FBI 19 and 58. See Mem. Op. at 16.

F. (U) Briefing Materials and Talking Points.

109. (U) Within this category, the Court has requested further justification with respect to the withholding of the following documents: OLC 7, 46, 65, 80, 81, 82, 84, 116, 125, 126, 134, and 202; ODAG 34, 41 and 54; and OIPR 13 and 137.

110. (U) With four exceptions, all of the briefing materials and talking points withheld by OLC in this category were prepared for internal use only in the course of briefings by Department staff for higher level officials or for use in meetings or discussions with official from elsewhere in the Government. With the exception of OLC 84, OLC 116, OLC 201, and OIPR 60, discussed further below, none of these materials was prepared for public briefing or discussion, and, again with the same four exceptions, none was adopted as official positions in subsequent public discussion of the TSP. Accordingly, as explained in my previous declaration, these briefing materials and talking points are by their very nature deliberative, as they reflect an attempt by the drafters succinctly to summarize particular issues and provide key background information in an effort to anticipate questions or issues

that may be raised at a briefing or other situation in which such documents are used. These materials provide concise summaries of information necessary for informed discussion of particular issues and attempt to anticipate and respond to questions that might be raised in any particular setting. Thus, these materials reflect the exchange of ideas and suggestions that accompanies all decisionmaking, and in many cases they also reflect assessments by attorneys and other staff about issues on which they have been asked to make recommendations or provide advice.

OLC 7

111. (U) OLC 7 consists of two copies of a one-page document. In reviewing OLC 7 in the course of preparing this declaration, I have determined that it contains information that originated with the NSA and thus should have been referred to NSA along with OLC's other referrals. The document has now been referred to NSA, and I understand that NSA will address the proper withholding of OLC 7 in its separate supplemental submission made in response to the Court's Order of September 5, 2007.

OLC 46

112. (U) OLC 46 consists of two copies of an undated one-page document entitled "Talkers," and a related electronic file, containing talking points that were created within the Department to assist senior administration officials in addressing various points about the TSP in internal discussions. This document is properly withheld under FOIA's Exemptions One, Three, and Five.

(U) Applicability of Exemptions One & Three.

113. **REDACTED**

(U) Applicability of Exemption Five.

114. (U) OLC 46 appears to have been created to provide high level Department officials with a concise summary of information that might be required for an internal meeting or a presentation. As described in my earlier declaration, briefing materials and talking points are by their very nature deliberative, as they reflect “an attempt by the drafters to succinctly summarize particular issues and provide key background information in an effort to anticipate questions or issues that may be raised at a briefing or other situation in which such documents are used” and reflect only “draft answers [that] may or may not be used or may be modified by the speakers in any particular setting.” Bradbury Decl. ¶ 73. For the reasons given in my prior declaration, OLC 46 is properly considered deliberative and pre-decisional, and thus exempt from disclosure under FOIA’s Exemption Five.

OLC 65

115. (U) OLC 65 is a five-page document (plus an electronic file), dated March 30, 2004, entitled “Briefing for AG.” This outline for a briefing to be provided to the Attorney General by the Deputy Attorney General prepared by Department staff includes a summary of preliminary OLC conclusions concerning the TSP and other intelligence activities; a discussion of issues for decision concerning these intelligence activities; a description of advice provided by OLC to other Executive Branch agencies and components concerning these activities; and an identification of legal issues requiring further discussion. OLC 65 is withheld pursuant to FOIA Exemptions One, Three, and Five.

Applicability of Exemption One & Three.

116. (U) OLC 65 contains classified information relating to the operation of the TSP and other intelligence activities that would be compromised by disclosure. For the reasons identified in my earlier declaration, see Bradbury Decl. ¶¶ 21-23, and in the

declaration of the former Director of National Intelligence, see DNI Decl. ¶¶ 22, 27-35, such information cannot be publicly disclosed without causing exceptionally grave harm to the national security of the United States.

117. **REDACTED**

Applicability of Exemption Five.

118. (U) OLC 65 is an internal briefing outline, which summarizes information compiled by Department staff for purposes of ensuring that higher level officials have the information necessary adequately to understand issues being presented to them for decision, which is protected by the deliberative process privilege. Disclosure of internal communications such as OLC 65 would identify the factors considered by Department decisionmakers in the course of their deliberations about intelligence activities and would impermissibly interfere with the provision of candid and concise summaries of critical information and recommendations to higher level Department officials by Department staff. OLC 65, accordingly, is properly exempt from disclosure under the deliberative process component of FOIA's Exemption Five.

OLC 80

119. (U) OLC 80 consists of six copies of an undated two-page document entitled "Technical Operation of [REDACTED],"⁴ some with handwritten notes and marginalia. These documents are withheld under FOIA Exemptions One, Three and Five.

(U) Applicability of Exemptions One & Three

120. (U) OLC 80 contains a detailed description of the operation of the TSP and other classified foreign intelligence activities and thus falls squarely within the category of "information that would reveal or tend to reveal operational details concerning the technical

⁴ (U) A classified codename is redacted.

methods by which NSA intercepts communications under the TSP,” which the former DNI identified as information that must be protected from disclosure. DNI Decl. ¶ 27. As the former DNI explained, “[d]etailed knowledge of the methods and practice of the U.S. Intelligence Community agencies must be protected from disclosure because such knowledge would be of material assistance to those who would seek to penetrate, detect, prevent, or damage the intelligence efforts of the United States, including efforts by this country to counter international terrorism.” *Id.* Information falling within this category, accordingly, including OLC 80, is properly protected as both classified and subject to the DNI’s authority to protect intelligence sources and methods. OLC 80, thus, is properly withheld under FOIA Exemptions One and Three.

121. **REDACTED**

122. **REDACTED**

(U) Applicability of Exemption Five.

123. (U) As described in my prior declaration, OLC 80 is a briefing paper that was created within the Department to assist senior Administration officials in addressing various points about the TSP. *See* Bradbury Decl. ¶ 73. This document was used for purposes of internal deliberations only; it was not prepared for purposes of providing information to the public. Briefing materials are by their very nature deliberative, as they reflect an attempt by the drafters succinctly to summarize particular issues and provide key background information in an effort to anticipate questions or issues that may be raised at a briefing or other situation in which such documents are used. *See id.* ¶ 80. OLC 80 reflects assessments by OLC attorneys about the relative importance of information considered necessary for purposes of briefing senior Administration officials, and the details of the information that need to be conveyed in any particular circumstance. To disclose such assessments would

harm the Department's deliberative process, and thus OLC 80 is properly withheld under FOIA's Exemption Five.

OLC 81 and OLC 82

124. (U) OLC 81 consists of 11 copies, some drafts and some with handwritten marginalia and notes, of four pages of briefing notes, dated December 18, 2005, which describe the TSP and other foreign intelligence activities and summarize various OLC legal opinions related to foreign intelligence collection activities. OLC 81 is withheld pursuant to FOIA Exemptions One, Three, and Five.

125. (U) OLC 82 consists of 20 copies, some drafts and some with handwritten edits and marginalia, plus eight related electronic files of a briefing outline, dated January 6, 2006, summarizing various topics related to foreign intelligence activities. OLC 82 is withheld pursuant to FOIA Exemptions One, Three, and Five.

Applicability of Exemption One & Three.

126. (U) OLC 81 and OLC 82 contain classified information relating to the scope and operation of the TSP and other intelligence activities that would be compromised by disclosure of these documents. For the reasons identified in my earlier declaration, see Bradbury Decl. ¶¶ 21-23, and in the declaration of the former Director of National Intelligence, see DNI Decl. ¶ 22, 27-35, such information cannot be publicly disclosed without causing exceptionally grave harm to the national security of the United States.

Applicability of Exemption Five.

127. (U) OLC 81 and OLC 82 are internal briefing outlines, created by my staff at my request and for my use, intended to be used to prepare me to brief others within the Government on issues concerning the TSP and other foreign intelligence activities. Specifically, OLC 81 was created so that I could brief Department officials regarding foreign

intelligence activities and OLC views following the publication of the article in The New York Times which divulged without authorization classified information concerning the TSP. OLC 82 was created as an outline for my use in the course of briefing members of the FISC. These documents contain recommendations from my staff as to topics for discussion, and are both deliberative and predecisional in the sense that, as I spoke in these meetings, I made the ultimate decision regarding which points would be made in any particular context. Disclosure of these documents would impermissibly interfere with my ability to ask my staff to create candid and concise summaries of critical information and recommendations for my use in discussions with higher level Department officials or other officials within the Government and, thus, would interfere with my ability to fulfill my official duties. OLC 81 and OLC 82, accordingly, are properly exempt from disclosure under the deliberative process component of FOIA's Exemption Five.

OLC 84

128. (U) OLC 84 is a nonfinal draft of a set of talking points, which was released to the public in final form on January 19, 2007, in a document entitled "Legal Authorities for the Recently Disclosed NSA Activities." The final version of this document is available on the Department's Internet site, www.usdoj.gov, and was provided to plaintiffs in response to their FOIA requests. It is my understanding that plaintiffs do not contest OLC's determination to withhold drafts, and thus this document is not further discussed herein.

OLC 116, OLC 201 & OIPR 60

129. (U) OLC 116, OLC 201, and OIPR 60 consist of nonfinal drafts of the Department's January 19, 2007, White Paper, which was released by the Department to the public in its final form, see www.usdoj.gov, and provided to plaintiffs in response to their

FOIA requests. It is my understanding that plaintiffs do not contest OLC's determination to withhold drafts, and thus these documents are not further discussed herein.

OLC 125, OLC 126, and OIPR 13

130. (U) OLC 125 is an undated two-page document entitled "Presentation: Where DOJ is on [REDACTED]." ⁵ This document is withheld under FOIA Exemptions One, Three, and Five.

131. (U) OLC 126 consists of two copies of a five-page document, dated March 14, 2004, which consists of bullet points related to OLC 125. This document is also withheld under FOIA Exemptions One, Three, and Five.

132. (U) OIPR 13 is a duplicate of OLC 126, and is withheld for the same reasons that apply to that record.

(U) Applicability of Exemptions One & Three.

133. REDACTED

(U) Applicability of Exemption Five.

134. (U) OLC 125 and OLC 126 contain preliminary legal analysis of OLC. The disclosure of such preliminary analysis would have the effect of discouraging thoughtful analysis of difficult legal questions as well as discouraging the creation of documents that set forth such preliminary analysis in order to assist in the process of developing final views. Disclosure of OLC's preliminary analysis, accordingly, would cause harm to the deliberative process by which OLC attorneys review legal issues and reach conclusions about them. Accordingly, OLC 125 and OLC 126 are exempt from disclosure under FOIA under the deliberative process privilege incorporated into Exemption Five.

⁵ (U) A classified codename is redacted.

135. (U) In addition, OLC 125 and OLC 126 were prepared for purposes of providing legal assistance and advice to other Executive Branch officials concerning DOJ's views about foreign intelligence activities. Disclosure of such advice would interfere with the attorney-client relationship between DOJ and other Executive Branch agencies and would discourage requests for timely and fully informed legal advice. Accordingly, OLC 125 and OLC 126 are protected by the attorney-client privilege, and are properly exempt under FOIA's Exemption Five for this reason as well.

OLC 134

136. (U) OLC 134 consists of three copies of a six-page set of attorney notes in bullet point form describing options to be considered in pending litigation before the FISC.

Applicability of Exemptions One and Three.

137. (U) OLC 134 is a set of attorney notes in bullet point form that should have been included in the category of documents described in my original declaration as category D. See Bradbury Decl. ¶¶ 54-59. It is my understanding that the court has entered summary judgment as to all of the documents in that category, see Mem. Op. at 15. OLC 134 is properly withheld for the same reasons. See Bradbury Decl. ¶¶ 54-59.

138. **REDACTED**

Applicability of Exemption Five

139. (U) OLC 134 is both deliberative and predecisional in that it consists of a list of options to be considered in pending litigation before the FISC. Thus, the document is protected by the deliberative process privilege and is properly withheld under Exemption Five of FOIA. In addition, OLC 134 is protected by the attorney work product doctrine in that it constitutes notes of an attorney concerning options that might be available in the

context of pending litigation and, thus, OLC 134 is properly withheld in its entirety under Exemption Five for this reason as well.

OLC 202

140. (U) OLC 202 is a set of draft talking points on legal matters which were not located in final form in OLC's classified files. It is my understanding that plaintiffs do not contest OLC's determination to withhold drafts and, thus, this document is not further discussed herein.

ODAG 34

141. (U) ODAG 34 is a duplicate of OLC 80 and is withheld for the reasons explained in paragraphs 123-27, supra.

ODAG 41

142. (U) ODAG 41 is a duplicate of OLC 125 and is withheld for the reasons explained in paragraphs 130, 133-35, supra.

ODAG 54

143. (U) ODAG 54 is a duplicate of OLC 46 and is withheld for the reasons explained in paragraphs 112-14, supra.

OIPR 13

144. (U) OIPR 13 is a duplicate of OLC 126 and is withheld for the reasons explained in paragraphs 131-35, supra.

OIPR 137

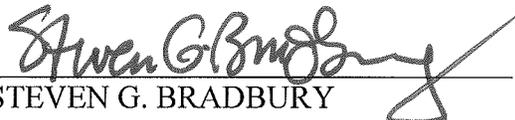
145. (U) OIPR 137 is a duplicate of OLC 65 and is withheld for the reasons explained in paragraphs 115-18, supra.

* * *

146. (U) Finally, the Court has requested clarification concerning the entries identified as OLC 95 and OLC 153-199 on the exhibit (Exhibit K) provided in support of my previous declaration, which were marked “intentionally left blank.” These identifiers were either not assigned to any document, were assigned to documents that were determined to be duplicative and thus removed from the index, or were assigned to documents that were determined during administrative review to be nonresponsive to plaintiffs’ requests. Accordingly, no responsive documents bear the designations OLC 95 or OLC 153-199.

I declare under penalty of perjury that the foregoing is true and correct.

Dated: October 18, 2007


STEVEN G. BRADBURY
Principal Deputy Assistant Attorney General
Office of Legal Counsel



U.S. Department of Justice

Office of Legal Counsel

Office of the Deputy Assistant Attorney General

Washington, D.C. 20530

May 17, 2002

Judge Colleen Kollar-Kotelly
U.S. District Court for the District of Court
U.S. Courthouse
3d & Constitution Ave., N.W.
Washington, D.C. 20001

Dear Judge:

It was a pleasure to meet you today. I am writing this letter, at the direction of the Attorney General and in the interests of comity between the executive and legislative branches, to follow up on your questions concerning the scope of the President's authority to conduct warrantless searches. In particular, this letter discusses the President's power to deploy expanded electronic surveillance techniques in response to the terrorist attacks against the United States on September 11, 2001. This letter outlines the legal justifications for such surveillance, which could be conducted without a warrant for national security purposes. Under the current circumstances, in which international terrorist groups continue to pose an immediate threat, we have concluded that such surveillance would be reasonable under the Fourth Amendment because it advances the compelling government interest of protecting the Nation from direct attack.

Part I of this memorandum discusses the relevant factual background. Part II examines the legal framework that governs the collection of electronic communications in the United States, and whether warrantless electronic surveillance is consistent with it. Part III reviews different doctrines that affect the legality of different types of surveillance. Part IV discusses the application of the Fourth Amendment in light of the September 11 attacks.

I.

Four coordinated terrorist attacks took place in rapid succession on the morning of September 11, 2001, aimed at critical Government buildings in the Nation's capital and landmark buildings in its financial center. Terrorists hijacked four airplanes: one then crashed into the Pentagon and two in the World Trade Center towers in New York City, the fourth, which was headed towards Washington, D.C., crashed in

~~TOP SECRET//ICS//SI//ORCON//NOFORN~~

JA393

~~TOP SECRET//ICS//SI//ORCON//NOFORN~~

Pennsylvania after passengers attempted to regain control of the aircraft. The attacks caused about five thousand deaths and thousands more injuries. Air traffic and communications within the United States have been disrupted; national stock exchanges were shut for several days; damage from the attack has been estimated to run into the billions of dollars. The President has found that these attacks are part of a violent terrorist campaign against the United States by groups affiliated with Al-Qaeda, an organization headed by Usama bin Laden, that includes the suicide bombing attack on the U.S.S. Cole in 2000, the bombing of our embassies in Kenya and Tanzania in 1998, the attack on a U.S. military housing complex in Saudi Arabia in 1996, and the bombing of the World Trade Center in 1993. The nation has undergone an attack using biological weapons, in which unknown terrorists have sent letters containing anthrax to government and media facilities, and which have resulted in the closure of executive, legislative, and judicial branch buildings.

In response, the Government has engaged in a broad effort at home and abroad to counter terrorism. Pursuant to his authorities as Commander-in-Chief and Chief Executive, the President has ordered the Armed Forces to attack al-Qaeda personnel and assets in Afghanistan, and the Taliban militia that harbors them. Congress has provided its support for the use of force against those linked to the September 11, 2001 attacks, and has recognized the President's constitutional power to use force to prevent and deter future attacks both within and outside the United States. S.J. Res. 23, Pub. L. No. 107-40, 115 Stat. 224 (2001). The military has also been deployed domestically to protect sensitive government buildings and public places from further terrorist attack. The Justice Department and the FBI have launched a sweeping investigation in response to the September 11 attacks. In October, 2001, Congress enacted legislation to expand the Justice Department's powers of surveillance against terrorists. By executive order, the President has created a new office for homeland security within the White House to coordinate the domestic program against terrorism.

Electronic surveillance techniques would be part of this effort. The President would order warrantless surveillance in order to gather intelligence that would be used to prevent and deter future attacks on the United States. Given that the September 11 attacks were launched and carried out from within the United States itself, an effective surveillance program might include individuals and communications within the continental United States. This would be novel in two respects. Without access to any non-public sources, it is our understanding that generally the National Security Agency (NSA) only conducts electronic surveillance of communications outside the United States that do not involve United States persons. Usually, surveillance of communications by United States persons within the United States is conducted by the FBI pursuant to a warrant obtained under the Foreign Intelligence Surveillance Act ("FISA"). Second, interception could include electronic messages carried through the internet, which again could include communications within the United States involving United States persons. Currently, it is our understanding that neither the NSA nor law enforcement conducts broad monitoring of electronic communications in this manner within the United States, without specific authorization under FISA.

~~TOP SECRET//ICS//SI//ORCON//NOFORN~~

II.

This Part discusses the legal authorities that govern the intelligence agencies, and whether warrantless electronic surveillance is consistent with them. Section A concludes that while certain aspects of such electronic surveillance might be inconsistent with earlier executive order, a presidential decision to conduct the surveillance constitutes a legitimate waiver to the order and is not unlawful. Section B concludes that the Foreign Intelligence Surveillance Act (“FISA”) does not restrict the constitutional authority of the executive branch to conduct surveillance of the type at issue here.

A.

The NSA was formed in 1952 by President Truman as part of the Defense Department. Under Executive Order 12,333, 46 Fed. Reg. 59941 (1981), the NSA is solely responsible for “signals intelligence activities [“SIGINT”].” Id. § 1.12(b)(1). It provides intelligence information acquired through the interception of communications to the White House, executive branch agencies, the intelligence community, and the armed forces for intelligence, counter-intelligence, and military purposes. Clearly, the basic authority for the establishment of the NSA is constitutional: the collections of SIGINT is an important part of the Commander-in-Chief and Chief Executive powers, which enable the President to defend the national security both at home and abroad. While Congress has enacted statutes authorizing the funding and organization of the NSA, it has never established any detailed statutory charter governing the NSA’s activities. See Intelligence Authorization Act for FY 1993, Pub. L. No. 102-496, sec. 705 (giving Secretary of Defense responsibility to ensure, through the NSA, the “continued operation of an effective unified organization for the conduct of signals intelligence activities”).

The NSA generally has limited its operations to the interception of international communications in which no United States person (a United States citizen, permanent resident alien, a U.S. corporation, or an unincorporated association with a substantial number of members who are U.S. citizens or permanent resident aliens) is a participant. According to publicly-available information, the NSA pulls in a great mass of international telephone, radio, computer, and other electronic communications, and then filters them using powerful computer systems for certain words or phrases. See, e.g., *Halkin v. Helms*, 690 F.2d 977, 983-84 (D.C. Cir. 1982). Congress, however, has not imposed any express statutory restrictions on the NSA’s ability to intercept communications that involve United States citizens or that occur domestically. This lack of limitations can be further inferred from the National Security Act of 1947. The Act places a clear prohibition, for example, upon the Central Intelligence Agency’s domestic activities. While Section 103 of the National Security Act commands the Director of Central Intelligence to “collect intelligence through human sources and by other appropriate means,” it also adds “except that the Agency shall have no police, subpoena, or law enforcement powers or internal security functions.” 50 U.S.C. § 403-3(d)(1) (1994 & Supp. V 1999). There is no similar provision that applies to the NSA, which implies that the NSA can conduct SIGINT operations domestically.

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

Rather than from statute, the limitation on the NSA's domestic SIGINT capabilities derives from executive order. Executive Order 12,333 requires that any "[c]ollection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the FBI." Executive Order 12,333, at § 2.3(b). If "significant foreign intelligence is sought," the Executive Order permits other agencies within the intelligence community to collect information "provided that no foreign intelligence collection by such agencies may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons." *Id.* Section 2.4 further makes clear that the intelligence community cannot use electronic surveillance, among other techniques, "within the United States or directed against United States persons abroad" unless they are according to procedures established by the agency head and approved by the Attorney General. In its own internal regulations, the NSA apparently has interpreted these provision as limiting its SIGINT operations only to international communications that do not involve United States persons.

Thus, the question arises whether a presidential decision to conduct warrantless electronic surveillance, for national security purposes, violates Executive Order 12,333, if such surveillance is not limited only to foreign communications that do not involve U.S. citizens. Thus, for example, all communications between United States persons, whether in the United States or not, and individuals in [REDACTED] might be intercepted. The President might direct the NSA to intercept communications between suspected terrorists, even if one of the parties is a United States person and the communication takes place between the United States and abroad. The non-content portion of electronic mail communications also might be intercepted, even if one of parties is within the United States, or one or both of the parties are non-citizen U.S. persons (i.e., a permanent resident alien). Such operations would expand the NSA's functions beyond the monitoring only of international communications of non-U.S. persons.

B1
B3

While such surveillance may go well beyond the NSA's current operations, it would not violate the text of the Executive Order. Executive Order 12,333 states that "when significant foreign intelligence is sought," the NSA and other agencies of the intelligence community may collect foreign intelligence within the United States. The only qualification on domestic collection is that it cannot be undertaken to acquire information about the domestic activities of United States persons. If United States persons were engaged in terrorist activities, either by communicating with members of Al Qaeda [REDACTED] or by communicating with foreign terrorists even within the United States, they are not engaging in purely "domestic" activities. Instead, they are participating in foreign terrorist activities that have a component within the United States. We do not believe that Executive Order 12,333 was intended to prohibit intelligence agencies from tracking international terrorist activities, solely because terrorists conduct those activities within the United States. This would create the odd incentive of providing international terrorists with more freedom to conduct their illegal activities *inside* the United States than outside of it. Rather, the Executive Order was meant to protect the privacy of United States persons where foreign threats were not involved. Further, Section 2.4 of Executive Order 12,333 contemplates that the NSA and other

B1
B3

~~TOP SECRET//ICS//SI//ORCON//NOFORN~~

intelligence agencies can collect intelligence within the United States, so long as the Attorney General approves the procedures.

Even if surveillance were to conflict with Executive Order 12,333, it could not be said to be illegal. An executive order is only the expression of the President's exercise of his inherent constitutional powers. Thus, an executive order cannot limit a President, just as one President cannot legally bind future Presidents in areas of the executive's Article II authority. Further, there is no constitutional requirement that a President issue a new executive order whenever he wishes to depart from the terms of a previous executive order. In exercising his constitutional or delegated statutory powers, the President often must issue instructions to his subordinates in the executive branch, which takes the form of an executive order. An executive order, in no sense then, represents a command from the President to himself, and therefore an executive order does not commit the President himself to a certain course of action. Rather than "violate" an executive order, the President in authorizing a departure from an executive order has instead modified or waived it. Memorandum for the Attorney General, From: Charles J. Cooper, Assistant Attorney General, *Re: Legal Authority for Recent Covert Arms Transfers to Iran* (Dec. 17, 1986). In doing so, he need not issue a new executive order, rescind the previous order, or even make his waiver or suspension of the order publicly known. Thus, here, the October 4, 2001 Authorization, even if in tension with Executive Order 12,333, only represents a one-time modification or waiver of the executive order, rather than a "violation" that is in some way illegal.

B.

Although it would not violate either the statutory authority for the NSA's operations or Executive Order 12,333, warrantless electronic surveillance within the United States, for national security purposes, would be in tension with FISA. FISA generally requires that the Justice Department obtain a warrant before engaging in electronic surveillance within the United States, albeit according to lower standards than apply to normal law enforcement warrants. Indeed, some elements of an electronic surveillance program – such as intercepting the communications of individuals for which probable cause exists to believe are terrorists – could probably be conducted pursuant to a FISA warrant. Here, however, a national security surveillance program could be inconsistent with the need for secrecy, nor would it be likely that a court could grant a warrant for other elements of a surveillance program, such as the monitoring of all calls to and from a foreign nation, or the general collection of communication addressing information. Nonetheless, as our Office has advised before, and as the Justice Department represented to Congress during passage of the Patriot Act of 2001, which resulted in several amendments to FISA, FISA only provides a safe harbor for electronic surveillance, and cannot restrict the President's ability to engage in warrantless searches that protect the national security. Memorandum for David S. Kris, Associate Deputy Attorney General, from John C. Yoo, Deputy Assistant Attorney General, *Re: Constitutionality of Amending Foreign Intelligence Surveillance Act to Change the "Purpose" Standard for Searches* (Sept. 25, 2001). The

~~TOP SECRET//ICS//SI//ORCON//NOFORN~~

ultimate test of the October 4 Authorization, therefore, is not FISA but the Fourth Amendment itself.

FISA requires that in order to conduct electronic surveillance for foreign intelligence purposes, the Attorney General must approve an application for a warrant, which is then presented to a special Article III court. If the target of the surveillance is a foreign power, the application need not detail the communications sought or the methods to be used. If the target is an agent of a foreign power, which the statute defines to include someone who engages in international terrorism, 50 U.S.C. § 1801(b)(2)(C) (1994 & Supp. V 1999), the application must contain detailed information concerning the target's identity, the places to be monitored, the communications sought, and the methods to be used. *Id.* at § 1804(a)(3)-(11). After passage of the FISA amendments as part of the Patriot Act, the National Security Adviser must certify that a "significant" purpose of the surveillance is to obtain foreign intelligence information that cannot be obtained through normal investigative techniques. FISA defines foreign intelligence information to include information that relates to "actual or potential attack or other grave hostile acts of a foreign power" or its agent, or information concerning "sabotage or international terrorism" by a foreign power or its agent, or information that, if a United States person is involved, is necessary for the national security or conduct of foreign affairs. *Id.* at § 1801(e).

FISA provides more secrecy and a lower level of proof for warrants. FISA creates a lesser standard than required by the Fourth Amendment for domestic law enforcement warrants, because the Attorney General need not demonstrate probable cause of a crime. He must only show that there is reason to believe that the target is a foreign power or an agent of a foreign power, and that the places to be monitored will be used by them. *Id.* at § 1804(a)(4)(A)-(B). If the target is a United States person, however, the Court must find that the National Security Adviser's certification is not clearly erroneous.

We do not believe an electronic surveillance program, undertaken in response to the September 11, 2001 attacks, could fully satisfy FISA standards. Such a program could seek to intercept all communications between the United States and certain countries where terrorist groups are known to operate, or communications that involve terrorists as participants. An effective surveillance program might not be able to enforce a distinction between United States persons or aliens, or to require that there be any actual knowledge of the identity of the targets of the search. FISA, however, requires that the warrant application identify the target with some particularity, probably either by name or by pseudonym. *Id.* at § 1804(a)(3); *cf. United States v. Principie*, 531 F.2d 1132 (2d Cir. 1976). To the extent that a presidential order would require probable cause to believe that a participant in a communication is a terrorist, this would more than meet FISA standards that the Justice Department show that the subject of a search is an agent of a foreign power. A standard based on reasonable grounds also would probably meet FISA standards. This, however, would not save a surveillance program's interception of all communications between the United States and another country from statutory difficulties.

Further problems are presented by FISA's requirement that the application describe the "places"

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

or "facilities" that are to be used by the foreign agent. While this requirement clearly extends beyond specific communication nodes, such as phones, to include facilities, we believe it unlikely that FISA would allow surveillance [REDACTED] Title III of the 1968 Act, for example, also requires the specification of "facilities" in addition to "places," and defines them as devices that transmit communications between two points. The courts have read "facilities" to allow surveillance of multiple telephone lines, rather than just an individual phone. We have not found an example, however, in which a court has granted a Title III warrant that would cover [REDACTED] which is the object of the surveillance program contemplated here. Thus, it is unlikely that the FISA court would grant a warrant that could authorize an effective surveillance program undertaken in response to the September 11 attacks.

FISA purports to be the exclusive statutory means for conducting electronic surveillance for foreign intelligence, just as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, claims to be the exclusive method for authorizing domestic electronic surveillance for law enforcement purposes. FISA establishes criminal and civil sanctions for anyone who engages in electronic surveillance, under color of law, except as authorized by statute, warrant, or court order. 50 U.S.C. § 1809-10. It might be thought, therefore, that a warrantless surveillance program, even if undertaken to protect the national security, would violate FISA's criminal and civil liability provisions.

Such a reading of FISA would be an unconstitutional infringement on the President's Article II authorities. FISA can regulate foreign intelligence surveillance only to the extent permitted by the Constitution's enumeration of congressional authority and the separation of powers. FISA itself is not required by the Constitution, nor does it necessarily establish standards and procedures that exactly match those required by the Fourth Amendment. Memorandum for David S. Kris, Associate Deputy Attorney General, from John C. Yoo, Deputy Assistant Attorney General, *Re: Constitutionality of Amending Foreign Intelligence Surveillance Act to Change the "Purpose" Standard for Searches* (Sept. 25, 2001); *cf.* Memorandum for Michael Vatis, Deputy Director, Executive Office for National Security, from Walter Dellinger, Assistant Attorney General, *Re: Standards for Searches Under Foreign Intelligence Surveillance Act* (Feb. 14, 1995). Instead, like the warrant process in the normal criminal context, FISA represents a statutory procedure that creates a safe harbor for surveillance for foreign intelligence purposes. If the government obtains a FISA warrant, its surveillance will be presumptively reasonable under the Fourth Amendment. Nonetheless, as we explained to Congress during passage of the Patriot Act, the ultimate test of whether the government may engage in foreign surveillance is whether the government's conduct is consistent with the Fourth Amendment, not whether it meets FISA.

This is especially the case where, as here, the executive branch possess the inherent constitutional power to conduct warrantless searches for national security purposes. Well before FISA's enactment, Presidents have consistently asserted—and exercised—their constitutional authority to conduct warrantless

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

searches necessary to protect the national security.¹ This Office has maintained, across different administrations controlled by different political parties, that the President's constitutional responsibility to defend the nation from foreign attack implies an inherent power to conduct warrantless searches. In 1995, we justified warrantless national security searches by recognizing that the executive branch needed flexibility in conducting foreign intelligence operations. Memorandum for Michael Vatis, Deputy Director, Executive Office for National Security, from Walter Dellinger, Assistant Attorney General, *Re: Standards for Searches Under Foreign Intelligence Surveillance Act* (Feb. 14, 1995). In 1980, we also said that "the lower courts – as well as this Department – have frequently concluded that authority does exist in the President to authorize such searches regardless of whether the courts also have the power to issue warrants for those searches. Memorandum for the Attorney General, from John M. Harmon, Assistant Attorney General, *Re: Inherent Authority* at 1 (Oct. 10, 1980).² FISA cannot infringe the President's inherent power under the Constitution to conduct national security searches, just as Congress cannot enact legislation that would interfere with the President's Commander-in-Chief power to conduct military hostilities. In either case, congressional efforts to regulate the exercise of an inherent executive power would violate the separation of powers by allowing the legislative branch to usurp the powers of the executive. *See* Memorandum for Timothy E. Flanigan, Deputy Counsel to the President, from John C. Yoo, Deputy Assistant Attorney General, *Re: The President's Constitutional Authority to Conduct Military Operations Against Terrorists and Nations Supporting Them* (Sept. 25, 2001) (War Powers Resolution cannot constitutionally define or regulate the President's Commander-in-Chief authority). Indeed, as we will see in Part IV, the Fourth Amendment's structure and Supreme Court case law demonstrate that the executive may engage in warrantless searches so long as the search is reasonable.

The federal courts have recognized the President's constitutional authority to conduct warrantless searches for national security purposes. To be sure, the Supreme Court has held that the warrant requirement should apply in cases of terrorism by purely domestic groups, *see United States v. United States District Court for the Eastern District of Michigan*, 407 U.S. 297, 299 (1972) ("Keith"), and has explicitly has not reached the scope of the President's surveillance powers with respect to the activities of foreign powers, *id.* at 308; *see also Katz. v. United States*, 389 U.S. 347, 358 n.23 (1967); *Mitchell*

¹A short description of this history is attached to this letter.

²Based on similar reasoning, this Office has concluded that the President could receive materials, for national defense purposes, acquired through Title III surveillance methods or grand juries. Memorandum for Frances Fragos Townsend, Counsel, Office of Intelligence Policy and Review, from Randolph D. Moss, Assistant Attorney General, *Re: Title III Electronic Surveillance Material and the Intelligence Community* (Oct. 17, 2000); Memorandum for Gerald A. Schroeder, Acting Counsel, Office of Intelligence Policy and Review, from Richard L. Shiffrin, Deputy Assistant Attorney General, *Re: Grand Jury Material and the Intelligence Community* (Aug. 14, 1997); *Disclosure of Grand Jury Matters to the President and Other Officials*, 17 Op. O.L.C. 59 (1993).

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

v. Forsyth, 472 U.S. 511, 531 (1985). Nevertheless, even after *Keith* the lower courts have continued to find that when the government conducts a search for national security reasons, of a foreign power or its agents, it need not meet the same requirements that would normally apply in the context of criminal law enforcement, such as obtaining a judicial warrant pursuant to a showing of probable cause. *See, e.g., United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980); *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974); *United States v. Buck*, 548 F.2d 871 (9th Cir.), *cert. denied* 434 U.S. 890 (1977); *United States v. Butenko*, 494 F.2d 593 (en banc), *cert. denied*, 419 U.S. 881 (1974); *United States v. Clay*, 430 F.2d 165 (5th Cir. 1970), *rev'd on other grounds*, 403 U.S. 698 (1971). Indeed, even FISA – which does not require a showing of probable cause – represents congressional agreement with the notion that surveillance conducted for national security purposes is not subject to the same Fourth Amendment standards that apply in domestic criminal cases.

Truong Dinh Hung exemplifies the considerations that have led the federal courts to recognize the President's constitutional authority to conduct warrantless national security searches. Unlike the domestic law enforcement context, the President's enhanced constitutional authority in national security and foreign affairs justifies a freer hand in conducting searches without *ex ante* judicial oversight. As the Fourth Circuit found, "the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would . . . 'unduly frustrate' the President in carrying out his foreign affairs responsibilities." *Truong Dinh Hung*, 629 F.2d at 913. A warrant requirement would be inappropriate, the court observed, because it would limit the executive branch's flexibility in foreign intelligence, delay responses to foreign intelligence threats, and create the chance for leaks. *Id.* Further, in the area of foreign intelligence, the executive branch is paramount in its expertise and knowledge, while the courts would have little competence in reviewing the government's need for the intelligence information. *Id.* at 913-14. In order to protect individual privacy interests, however, the court limited the national security exception to the warrant requirement to cases in which the object of the search is a foreign power, its agents, or collaborators, and when the surveillance is conducted primarily for foreign intelligence reasons. *Id.* at 915. The other lower courts to have considered this question similarly have limited the scope of warrantless national security searches to those circumstances.

Here, it seems clear that the current environment falls within the exception to the warrant requirement for national security searches. Foreign terrorists have succeeded in launching a direct attack on important military and civilian targets within the United States. The President may find that terrorists constitute an ongoing threat against the people of the United States and their national government, and he may find that protecting against this threat is a compelling government interest. The government would be conducting warrantless searches in order to discover information that will prevent future attacks on the United States and its citizens. This surveillance may provide information on the strength of terrorist groups, the timing and methods of their attack, and the target. The fact that the foreign terrorists have operated, and may continue to operate, within the domestic United States, does not clothe their operations in the constitutional protections that apply to domestic criminal investigations. *See Memorandum for Alberto R.*

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

Gonzalez, Counsel to the President and William J. Haynes, II, General Counsel, Department of Defense, from John C. Yoo, Deputy Assistant Attorney General and Robert J. Delahunty, Special Counsel, Re: *Authority for Use of Military Force to Combat Terrorist Activities Within the United States* (Oct. 23, 2001). While some information might prove useful to law enforcement, the purpose of the surveillance program remains that of protecting the national security. As we have advised in a separate memorandum, a secondary law enforcement use of information, which was originally gathered for national security purposes, does not suddenly render the search subject to the ordinary Fourth Amendment standards that govern domestic criminal investigations. See Memorandum for David S. Kris, Associate Deputy Attorney General, from John C. Yoo, Deputy Assistant Attorney General, Re: *Constitutionality of Amending Foreign Intelligence Surveillance Act to Change the "Purpose" Standard for Searches* (Sept. 25, 2001).

Due to the President's paramount constitutional authority in the field of national security, a subject which we will discuss in more detail below, reading FISA to prohibit the President from retaining the power to engage in warrantless national security searches would raise the most severe of constitutional conflicts. Generally, courts will construe statutes to avoid such constitutional problems, on the assumption that Congress does not wish to violate the Constitution, unless a statute clearly demands a different construction. See, e.g., *Edward J. DeBartolo Corp. v. Florida Gulf Coast Building & Construction Trades Council*, 485 U.S. 568, 575 (1988). Unless Congress signals a clear intention otherwise, a statute must be read to preserve the President's inherent constitutional power, so as to avoid any potential constitutional problems. Cf. *Public Citizen v. Department of Justice*, 491 U.S. 440, 466 (1989) (construing Federal Advisory Committee Act to avoid unconstitutional infringement on executive powers); *Association of American Physicians & Surgeons v. Clinton*, 997 F.2d 898, 906-11 (D.C. Cir. 1993) (same). Thus, unless Congress made a clear statement in FISA that it sought to restrict presidential authority to conduct warrantless searches in the national security area – which it has not – then the statute must be construed to avoid such a reading. Even if FISA's liability provisions were thought to apply, we also believe that for a variety of reasons they could not be enforced against surveillance conducted on direct presidential order to defend the nation from attack. This issue can be discussed in more detail, if desired.

III.

Having established that the President has the authority to order the conduct of electronic surveillance without a warrant for national security purposes, we now examine the justification under the Fourth Amendment for the specific searches that might arise. The Fourth Amendment declares that "the right of the people to be secure in their persons, houses, papers, and effects, against *unreasonable* searches and seizures, shall not be violated." U.S. Const. amend IV. The Amendment also declares that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized." *Id.* This Part will discuss the reasons why several elements of a possible surveillance program would not even trigger Fourth Amendment

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

scrutiny because they would not constitute a “search” for constitutional purposes.

A.

Aspects of surveillance that do not involve United States persons and that occur extraterritorially do not raise Fourth Amendment concerns. As the Supreme Court has found, the Fourth Amendment does not apply to military or intelligence operations conducted against aliens overseas. *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990). In *Verdugo-Urquidez*, the Court found that the purpose of the Fourth Amendment “was to restrict searches and seizures which might be conducted by the United States in domestic matters. *Id.* at 266. As the Court concluded, the Fourth Amendment’s design was “to protect the people of the United States against arbitrary action by their own government; it was never suggested that the provision was intended to restrain the actions of the Federal Government against aliens outside of the United States territory.” *Id.* Indeed, the Court reversed a court of appeals’ holding that the Fourth Amendment applied extraterritorially because of its concern that such a rule would interfere with the nation’s military operations abroad:

The rule adopted by the Court of Appeals would apply not only to law enforcement operations abroad, but also to other foreign policy operations which might result in “searches or seizures.” The United States frequently employs Armed Forces outside this country—over 200 times in our history—for the protection of American citizens or national security Application of the Fourth Amendment to those circumstances could significantly disrupt the ability of the political branches to respond to foreign situations involving our national interest. Were respondent to prevail, aliens with no attachment to this country might well bring actions for damages to remedy claimed violations of the Fourth Amendment in foreign countries or in international waters. . . . [T]he Court of Appeals’ global view of [the Fourth Amendment’s] applicability would plunge [the political branches] into a sea of uncertainty as to what might be reasonable in the way of searches and seizures conducted abroad.

Id. at 273-74 (citations omitted). Here, the Court made clear that aliens had no Fourth Amendment rights to challenge activity by the United States conducted abroad.

Thus, as applied, elements of a surveillance program would not even raise Fourth Amendment concerns, because much of the communications that the NSA would intercept would be those of non-U.S. persons abroad. [REDACTED] for example, which themselves do not terminate or originate in the United States and do not involve a U.S. person, do not involve a “search or seizure” under the Fourth Amendment. Further, any communications between terrorists that occur wholly abroad, and in which none of the terrorist participants are U.S. persons, also do not trigger Fourth Amendment scrutiny. An even narrower program, which would limit the interception

B1
B3

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

of communications involving terrorists to those that originate or terminate outside the United States, further narrows the likelihood that communications between U.S. persons within the United States will be intercepted.

B.

Second, intercepting certain communications that move internationally may not raise a Fourth Amendment issue because of what is known as the “border search exception.” A surveillance program could direct the interception of all communications to or from another country in which terrorists are operating, which by definition would be international communication. Therefore, much if not all of the communications to be intercepted would cross the borders of the United States.

Under the border search exception to the Fourth Amendment, the federal government has the constitutional authority to search anything or anyone crossing the borders of the United States without violating any individual rights. In *United States v. Ramsey*, 431 U.S. 606 (1977), the Supreme Court upheld the constitutionality of searching incoming international mail based on reasonable cause to suspect that such mail contained illegally imported merchandise. Recognizing what it characterized as a “border search exception” to the Fourth Amendment’s warrant and probable cause requirements, the Court observed that “searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border.” *Id.* at 616. The Court made clear that the manner in which something or someone crossed the border made no difference. “It is clear that there is nothing in the rationale behind the border search exception which suggests that the mode of entry will be critical.” *Id.* at 620. The Court also observed that there was no distinction to be drawn in what crossed the border, “[i]t is their entry into this country from without it that makes a resulting search ‘reasonable.’” *Id.* Although the Supreme Court has not examined the issue, the lower courts have unanimously found that the border search exception also applies to the exit search of outgoing traffic as well.³

Based on this doctrine, the interception of international communications could be justified by analogizing to the border search of international mail. Although electronic mail is, in some sense, intangible, it is also a message that begins at a physical server computer and then, though the movement of digital signals across wires, is transmitted to another server computer in a different location. Electronic mail is just

³See, e.g., *United States v. Oriakhi*, 57 F.3d 1290 (4th Cir. 1995); *United States v. Berisha*, 925 F.2d 791 (5th Cir. 1991); *United States v. Ezeiruaku*, 936 F.2d 136 (3d Cir. 1991); *United States v. Nates*, 831 F.2d 860 (9th Cir. 1987), cert. denied, 487 U.S. 1205 (1988); *United States v. Hernandez-Salazar*, 813 F.2d 1126 (11th Cir. 1987); *United States v. Benevento*, 836 F.2d 60 (2d Cir. 1987), cert. denied, 486 U.S. 1043 (1988); *United States v. Udofot*, 711 F.2d 831 (8th Cir.), cert. denied, 464 U.S. 896 (1983).

~~TOP SECRET//ICS//SI//ORCON//NOFORN~~

a different method of transporting a communication across the border of the United States. As the Court emphasized in *Ramsey*, “[t]he critical fact is that the envelopes cross the border and enter this country, not that they are brought in by one mode of transportation rather than another.” *Id.* at 620. The fact that the method of transportation is electronic, rather than physical, should not make a difference, nor should it matter that the search does not occur precisely when the message crosses the nation’s borders. Indeed, searches of outbound or inbound international mail or luggage take place at facilities within the nation’s borders, after they have arrived by air, just as searches of electronic messages could occur once an international message appears on a server within the United States after transmission across our borders. It should be admitted that we have not found any cases applying *Ramsey* in this manner, although we also have not found any reported cases in which a court was confronted with a search effort of all international communications either.

There are three further caveats to raise in regard to the border search exception theory. First, it is altogether unclear whether *Ramsey* would apply at all to telephone conversations. While telephone conversations are like letters in that they convey messages, they are also ongoing, real-time transactions which do not contain discrete, self-contained chunks of communication. Second, and related to the first point, the Court has cautioned that examination of international mail for its content would raise serious constitutional questions. In *Ramsey*, the government opened outgoing mail that it suspected contained illegal drugs; regulations specifically forbade customs officials from reading any correspondence. Thus, the crime there was not the content of the communication itself, although the content could have been related to the transportation of the illegal substance. First Amendment issues would be raised if the very purpose of opening correspondence was to examine its content. *Id.* at 623-24. Third, the Court observed that serious constitutional problems in *Ramsey* were avoided due to a probable cause requirement. While this Office has advised that a reasonableness standard might still be constitutional if applied to international mail searches, we also acknowledged that our conclusion was not free from doubt. See Memorandum for Geoffrey R. Greiveldinger, Counsel for National Security Matters, Criminal Division, from Teresa Wynn Roseborough and Richard L. Shiffrin, Deputy Assistant Attorneys General, *Customs Service Proposal for Outbound Mail Search Authority, Amendment of Titles 31 U.S.C. § 5317(b) and 39 U.S.C. § 3623(d)* (Oct. 31, 1995). In light of these caveats, we can conclude that the border search exception would apply most squarely to the acquisition of communication addressing information, which for reasons we discuss below is not content, but might not reach the interception of the contents of telephone or other electronic communication.

C.

Third, the interception of electronic mail for its non-content information should not raise Fourth Amendment concerns. Capturing only the non-content addressing information of electronic communications may be analogized to a “pen register.” A pen register is a device that records the numbers dialed from a telephone. In *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court found that the

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

warrantless installation of a pen register for a defendant's home phone line did not violate the Fourth Amendment because use of a pen register was not a "search" within the meaning of the Amendment. Applying the test set out in *Katz v. United States*, 389 U.S. 347 (1967), the Court evaluated whether a person could claim a "legitimate expectation of privacy" in the phone numbers dialed. It found that a person could not have a legitimate expectation of privacy, because they should know that they numbers dialed are recorded by the phone company for legitimate business purposes, and that a reasonable person could not expect that the numerical information he voluntarily conveyed to the phone company would not be "exposed." *Id.* at 741-46. Because pen registers do not acquire the contents of communication, and because a person has no legitimate expectation of privacy in the numbers dialed, the Court concluded, use of a pen register does not constitute a search for Fourth Amendment purposes.

The Court's blessing of pen registers suggests that a surveillance program that sought only non-content information from electronic messages would be similarly constitutional. An interception program for electronic mail, for example, could capture only non-content information in regard to which a reasonable person might not have a legitimate expectation of privacy. E-mail addresses, like phone numbers, are voluntarily provided by the sender to the internet service provider (ISP) in order to allow the company to properly route the communication. A reasonable person could be expected to know that an ISP would record such message information for their own business purposes, just as telephone companies record phone numbers dialed. Furthermore, other information such as routing and server information is not even part of the content of a message written by the sender. Rather, such information is generated by the ISP itself, as part of its routine business operations, to help it send the electronic message through its network to the correct recipient. A sender could have no legitimate expectation of privacy over information he did not even include in his message, but instead is created by the ISP as part of its own business processes. A person would have no more privacy interest in that information than he would have in a postmark stamped onto the outside of an envelope containing his letter.

Whether a surveillance program involving electronic mail would sweep in content poses a more difficult question. From *Smith*, it appears that a pen register does not effectuate a Fourth Amendment search, in part, because it does not capture content from a communication. "Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed." *Smith*, 442 U.S. at 741. Here, it is no doubt true that electronic mail addressing information, created by the author of a communication, could contain some content. Variations of an addressee's name are commonly used to create e-mail addresses, and elements of the address can reveal other information, such as the institution or place someone works – hence, my e-mail address, assigned to me by the Justice Department, is john.c.yoo@usdoj.gov. This, however, does not render such information wholly subject to the Fourth Amendment. Even phone numbers can provide information that contains content. Phone numbers, for example, are sometimes used to spell words (such as 1-800-CALL-ATT), phone numbers can provide some location information, such as if someone calls a well-known hotel's number, and keypunches can even send messages, such as through pager systems. We believe that an individual's willingness to convey

~~TOP SECRET/HCS/SJ/ORCON/NOFORN~~

to an ISP addressing information, which the ISP then uses for its own business purposes, suggests that an individual has no legitimate expectation of privacy in the limited content that could be inferred from e-mail addresses. We also note, however, that the courts have yet to encounter this issue in any meaningful manner, and so we cannot predict with certainty whether the judiciary would agree with our approach.

It should be noted that Congress has recognized the analogy between electronic mail routing information and pen registers. It recently enacted legislation authorizing pen register orders for non-content information from electronic mail. See USA Patriot Act of 2001, Pub. L. No. 107-56, § 216. While Congress extended pen register authority to surveillance of electronic mail, it also subjected that authority to the general restrictions of Title III and FISA, which require the Justice Department to obtain an ex parte court order before using such devices. While the requirements for such an order are minimal, see 18 U.S.C. § 3122 (government attorney must certify only that information likely to be gained from pen register “is relevant to an ongoing criminal investigation being conducted by that agency”), a warrantless surveillance program would not seek a judicial order for the surveillance program here. Title III attempts to forbid the use of pen registers or, now, electronic mail trap and trace devices, without a court under Title III or FISA. *Id.* at § 3121(a). As with our analysis of FISA, however, we do not believe that Congress may restrict the President’s inherent constitutional powers, which allow him to gather intelligence necessary to defend the nation from direct attack. *See supra*. In any event, Congress’s belief that a court order is necessary before using a pen register does not affect the constitutional analysis under the Fourth Amendment, which remains that an individual has no Fourth Amendment right in addressing information. Indeed, the fact that use of pen register and electronic trap and trace devices can be authorized without a showing of probable cause demonstrates that Congress agrees that such information is without constitutional protections.

D.

Fourth, intelligence gathering in direct support of military operations does not trigger constitutional rights against illegal searches and seizures. Our Office has recently undertaken a detailed examination of whether the use of the military domestically in order to combat terrorism would be restricted by the Fourth Amendment. *See Memorandum for Alberto R. Gonzalez, Counsel to the President and William J. Haynes, II, General Counsel, Department of Defense, from John C. Yoo, Deputy Assistant Attorney General and Robert J. Delahunty, Special Counsel, Re: Authority for Use of Military Force to Combat Terrorist Activities Within the United States* (Oct. 23, 2001). While we will only summarize here our reasoning, it should be clear that to the extent that a surveillance program is aimed at gathering intelligence for the military purpose of using the Armed Forces to prevent further attacks on the United States, that activity in our view is not restricted by the Fourth Amendment.

As a matter of the original understanding, the Fourth Amendment was aimed primarily at curbing law enforcement abuses. Although the Fourth Amendment has been interpreted to apply to governmental actions other than criminal law enforcement, the central concerns of the Amendment are focused on police

~~TOP SECRET//ICS//SI//ORCON//NOFORN~~

activity. See, e.g., *South Dakota v. Opperman*, 428 U.S. 364, 370 n.5 (1976). As we will explain in further detail in Part IV below, the Court has recognized this by identifying a “special needs” exception to the Fourth Amendment’s warrant and probable cause requirements. See, e.g., *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646 (1995); *Indianapolis v. Edmond*, 531 U.S. 32 (2000). However well suited the warrant and probable cause requirements may be as applied to criminal investigation and law enforcement, they are unsuited to the demands of wartime and the military necessity to successfully prosecute a war against an enemy. In the circumstances created by the September 11 attacks, the Constitution provides the Government with expanded powers and reduces the restrictions created by individual civil liberties. As the Supreme Court has held, for example, in wartime the government may summarily requisition property, seize enemy property, and “even the personal liberty of the citizen may be temporarily restrained as a measure of public safety.” *Yakus v. United States*, 321 U.S. 414, 443 (1944) (citations omitted). “In times of war or insurrection, when society’s interest is at its peak, the Government may detain individuals whom the Government believes to be dangerous.” *United States v. Salerno*, 481 U.S. 739, 748 (1987); see also *Moyer v. Peabody*, 212 U.S. 78 (1909) (upholding detention without probable cause during time of insurrection) (Holmes, J.).

Because of the exigencies of war and military necessity, the Fourth Amendment should not be read as applying to military operations. In *Verdugo-Urquidez*, discussed in Part III, the Court made clear that the Fourth Amendment does not apply to military operations overseas. 494 U.S. at 273-274. As the Court observed, if things were otherwise, both political leaders and military commanders would be severely constrained by having to assess the “reasonableness” of any military action beforehand, thereby interfering with military effectiveness and the President’s constitutional responsibilities as Commander-in-Chief. It also seems clear that the Fourth Amendment would not restrict military operations within the United States against an invasion or rebellion. See, e.g., 24 Op. Att’y Gen. 570 (1903) (American territory held by enemy forces is considered hostile territory where civil laws do not apply). Were the United States homeland invaded by foreign military forces, our armed forces would have to take whatever steps necessary to repel them, which would include the “seizure” of enemy personnel and the “search” of enemy papers and messages, it is difficult to believe that our government would need to show that these actions were “reasonable” under the Fourth Amendment. The actions of our military, which might cause collateral damage to United States persons, would no more be constrained by the Fourth Amendment than if their operations occurred overseas. Nor is it necessary that the military forces on our soil be foreign. Even if the enemies of the Nation came from within, such as occurred during the Civil War, the federal Armed Forces must be free to use force to respond to such an insurrection or rebellion without the constraints of the Fourth Amendment. Indeed, this was the understanding that prevailed during the Civil War.

These considerations could justify much of a warrantless electronic surveillance program. Although the terrorists who staged the September 11, 2001 events operated clandestinely and have not occupied part of our territory, they have launched a direct attack on both the American homeland and our assets overseas that have caused massive casualties. Their attacks were launched and carried out from within the

~~TOP SECRET//ICS//SI//ORCON//NOFORN~~

United States itself. Pursuant to his authority as Commander-in-Chief and Chief Executive, the President has ordered the use of military force against the terrorists both at home and abroad, and he has found that they present a continuing threat of further attacks on the United States. Application of the Fourth Amendment could, in many cases, prevent the President from fulfilling his highest constitutional duty of protecting and preserving the Nation from direct attack. Indeed, the opposite rule would create the bizarre situation in which the President would encounter less constitutional freedom in using the military when the Nation is directly attacked at home, where the greatest threat to American civilian casualties lies, than we use force abroad.

Thus, the Fourth Amendment should not limit military operations to prevent attacks that take place within the American homeland, just as it would not limit the President's power to respond to attacks launched abroad. A surveillance program, undertaken for national security purposes, would be a necessary element in the effective exercise of the President's authority to prosecute the current war successfully. Intelligence gathered through surveillance allows the Commander-in-Chief to determine how best to position and deploy the Armed Forces. It seems clear that the primary purpose of the surveillance program is to defend the national security, rather than for law enforcement purposes, which might trigger Fourth Amendment concerns. In this respect, it is significant that the President would be ordering the Secretary of Defense (who supervises the NSA), rather than the Justice Department, to conduct the surveillance, and that evidence would not be preserved for later use in criminal investigations. While such secondary use of such information for law enforcement does not undermine the primary national security purpose motivating the surveillance program, it is also clear that such intelligence material, once developed, can be made available to the Justice Department for domestic use.

IV.

Even if a surveillance program, or elements of it, were still thought to be subject to Fourth Amendment scrutiny, we think that compelling arguments can justify its constitutionality. This Part will review whether warrantless electronic surveillance, undertaken for national security purposes, is constitutional under the Fourth Amendment. It should be clear at the outset that the Fourth Amendment does not require a warrant for every search, but rather that a search be "reasonable" to be constitutional. In light of the current security environment, the government can claim a compelling interest in protecting the nation from attack sufficient to outweigh any intrusion into privacy interests.

A.

The touchstone for review of a government search is whether it is "reasonable." According to the Supreme Court, "[a]s the text of the Fourth Amendment indicates the ultimate measure of the constitutionality of a governmental search is 'reasonableness.'" *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 652 (1995). When law enforcement undertakes a search to discover evidence of criminal

~~TOP SECRET//ICS//SI//ORCON//NOFORN~~

wrongdoing, the Supreme Court has said that reasonableness generally requires a judicial warrant on a showing of probable cause that a crime has been or is being committed. *Id.* at 653. But the Court has also recognized that a warrant is not required for all government searches, especially those that fall outside the ordinary criminal investigation context. A warrantless search can be constitutional “when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.” *Id.*

A variety of government searches, therefore, have met the Fourth Amendment’s requirement of reasonableness without obtaining a judicial warrant. The Supreme Court, for example, has upheld warrantless searches that involved the drug testing of high school athletes, *id.*, certain searches of automobiles, *Pennsylvania v. Labron*, 518 U.S. 938 (1996) (per curiam), drunk driver checkpoints, *Michigan v. Dep’t of State Police v. Sitz*, 496 U.S. 444 (1990), drug testing of railroad personnel, *Skinner v. Railway Labor Executives’ Ass’n*, 489 U.S. 602 (1989), drug testing of federal customs officers, *Treasury Employees v. Von Raab*, 489 U.S. 656 (1989), administrative inspection of closely regulated businesses, *New York v. Burger*, 482 U.S. 691 (1987); temporary baggage seizures, *United States v. Place*, 462 U.S. 696 (1983), detention to prevent flight and to protect law enforcement officers, *Michigan v. Summers*, 452 U.S. 692 (1981), checkpoints to search for illegal aliens, *United States v. Martinez-Fuerte*, 428 U.S. 543 (1976), and temporary stops and limited searches for weapons, *Terry v. Ohio*, 392 U.S. 1 (1968). The Court has cautioned, however, that a random search program cannot be designed to promote a general interest in crime control. *See Indianapolis v. Edmond*, 531 U.S. 32, 41 (2000); *Delaware v. Prouse*, 440 U.S. 648, 659 n.18 (1979).

Reasonableness does not lend itself to precise tests or formulations. Nonetheless, in reviewing warrantless search programs, the Court generally has balanced the government’s interest against intrusion into privacy interests. “When faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable.” *Illinois v. McArthur*, 121 S. Ct. 946, 949 (2001). Or, as the Court has described it, warrantless searches may be justified if the government has “special needs” that are unrelated to normal law enforcement. In these situations, the Court has found a search reasonable when, under the totality of the circumstances, the “importance of the governmental interests” has outweighed the “nature and quality of the intrusion on the individual’s Fourth Amendment interests.” *Tennessee v. Garner*, 471 U.S. 1, 8 (1985).

B.

This analysis suggests that the Fourth Amendment would permit warrantless electronic surveillance if the government’s interest outweighs intrusions into privacy interests. It should be clear that the President’s directive falls within the “special needs” exception to the warrant requirement that calls for such a balancing test. The surveillance program is not designed to advance a “general interest in crime control,”

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

Edmond, 531 U.S. at 44, but instead seeks to protect the national security by preventing terrorist attacks upon the United States. As the national security search cases discussed in Part II recognize, defending the nation from foreign threats is a wholly different enterprise than ordinary crime control, and this difference justifies examination of the government's action solely for its reasonableness. Indeed, as the Supreme Court recognized in *Edmond*, warrantless, random searches undertaken for national security purposes, such as forestalling a terrorist attack on an American city, would be constitutional even if the same search technique, when undertaken for general crime control, would fail Fourth Amendment standards.

Applying this standard, we find that the government's interest here is perhaps of the highest order – that of protecting the nation from attack. Indeed, the factors justifying warrantless searches for national security reasons are more compelling now than at the time of the earlier lower court decisions discussed in Part II. While upholding warrantless searches for national security purposes, those earlier decisions had not taken place during a time of actual hostilities prompted by a surprise, direct attack upon civilian and military targets within the United States. A direct attack on the United States has placed the Nation in a state of armed conflict; defending the nation is perhaps the most important function of government. As the Supreme Court has observed, “It is ‘obvious and unarguable’ that no governmental interest is more compelling than the security of the Nation.” *Haig v. Agee*, 453 U.S. 280, 307 (1981). As Alexander Hamilton observed in *The Federalist*, “there can be no limitation of that authority, which is to provide for the defence and protection of the community, in any matter essential to its efficacy.” *The Federalist* No. 23, at 147-48 (Alexander Hamilton) (Jacob E. Cooke ed., 1961). If the situation warrants, the Constitution recognizes that the federal government, and indeed the President, must have the maximum power permissible under the Constitution to prevent and defeat attacks upon the Nation.

In authorizing an electronic surveillance program, the President should lay out the proper factual predicates for finding that the terrorist attacks had created a compelling governmental interest. The September 11, 2001 attacks caused thousands of deaths and even more casualties, and damaged both the central command and control facility for the Nation's military establishment and the center of the country's private financial system. In light of information that would be provided by the intelligence community and the military, the President could further conclude that terrorists continue to have the ability and the intention to undertake further attacks on the United States. Given the damage caused by the attacks on September 11, 2001, the President could judge that future terrorist attacks could cause massive damage and casualties and threatens the continuity of the federal government. He could conclude that such circumstances justify a compelling interest on the part of the government to protect the United States and its citizens from further terrorist attack. It seems certain that the federal courts would defer to the President's determination on whether the United States is threatened by attack and what measures are necessary to respond. *See, e.g., The Prize Cases*, 67 U.S. 635, 670 (1862) (decision whether to consider rebellion a war is a question to be decided by the President). These determinations rest at the core of the President's power as Commander-in-Chief and his role as representative of the Nation in its foreign affairs. *See United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304 (1936).

~~TOP SECRET//ICS//SI//ORCON//NOFORN~~

Under the Constitution's design, it is the President who is primarily responsible for advancing that compelling interest. The text, structure, and history of the Constitution establish that the President bears the constitutional duty, and therefore the power, to ensure the security of the United States in situations of grave and unforeseen emergency. *See generally* Memorandum for Timothy E. Flanigan, Deputy Counsel to the President, from John C. Yoo, Deputy Assistant Attorney General, *Re: The President's Constitutional Authority to Conduct Military Operations Against Terrorists and Nations Supporting Them* (Sept. 25, 2001). Both the Vesting Clause, U.S. Const. art. II, § 1, cl. 1, and the Commander in Chief Clause, *id.*, § 2, cl. 1, vest in the President the power to deploy military force in the defense of the United States. The Constitution makes explicit the President's obligation to safeguard the nation's security by whatever lawful means are available by imposing on him the duty to "take Care that the Laws be faithfully executed." *Id.*, § 3. The constitutional text and structure are confirmed by the practical consideration that national security decisions require a unity in purpose and energy in action that characterize the Presidency rather than Congress. As Alexander Hamilton explained, "[o]f all the cares or concerns of government, the direction of war most peculiarly demands those qualities which distinguish the exercise of power by a single hand." *The Federalist* No. 74, at 500 (Alexander Hamilton) (Jacob E. Cooke ed. 1961).

Surveillance initiated in response to the September 11 attacks would clearly advance this interest. The President would be exercising his powers as Commander-in-Chief and Chief Executive to direct military action against Al Qaeda and Taliban forces in Afghanistan, and to use the armed forces to protect United States citizens at home. Congress has approved the use of military force in response to the September 11 attacks. Pub. L. No. 107-40, 115 Stat. 224 (2001). It is well established that the President has the independent constitutional authority as Commander-in-Chief to gather intelligence in support of military and national security operations, and to employ covert means, if necessary, to do so. *See Totten v. United States*, 92 U.S. 105, 106 (1876). The President's "constitutional power to gather foreign intelligence," *Warrantless Foreign Intelligence Surveillance – Use of Television – Beepers*, 2 Op. O.L.C. 14, 15 (1978), includes the discretion to use the most effective means of obtaining information, and to safeguard those means. Intelligence gathering is a necessary function that enables the President to carry out these authorities effectively. The Commander-in-Chief needs accurate and comprehensive intelligence on enemy movements, plans, and threats in order to best deploy the United States armed forces and to successfully execute military plans. Warrantless searches could provide the most effective method, in the President's judgment, to obtain information necessary for him to carry out his constitutional responsibility to defend the Nation from attack.

By contrast, the intrusion into an individual citizen's privacy interests may not be seen as so serious as outweighing the government's most compelling of interests. The searches that would take place are as not as intrusive as those which occur when the government monitors the communications of a target in the normal Title III or FISA context. These often require an agent to consciously and actively listen in to telephone conversations. Here, as we understand it, [REDACTED]

B1
B3

~~TOP SECRET/HCS/SI/ORCON/NOFORN~~B1
B3

If privacy interests are viewed as intruded upon only by [REDACTED] it is likely that Fourth Amendment interests would not outweigh the compelling governmental interest present here. In the context of roadblocks to stop drunken drivers, another area of "special needs" under the Fourth Amendment, the Court has permitted warrantless searches. *See Michigan Dep't of State Police v. Sitz*, 496 U.S. 444 (1990). There, the Court found that a roadblock constituted a "reasonable" search due to the magnitude of the drunken driver problem and the deaths it causes – in fact, the court compared the death toll from drunk drivers to the casualties on a battlefield. *Id.* at 451. It found that this interest outweighed the intrusion into privacy at a checkpoint stop, which it characterized as "brief" in terms of duration and intensity. Similarly, [REDACTED]

B1
B3

[REDACTED] than in the case of a roadblock, where a [REDACTED] law enforcement officer stops each driver to examine whether they are inebriated. It seems that if the Supreme Court were willing to uphold drunk driver checkpoints, it would be equally or even more willing to allow [REDACTED]⁴

B1
B3B1
B3

The restriction of a surveillance program only to those communications which originate or terminate in a foreign country or which involve terrorists further reduces any possible intrusion into individual privacy interests. If probable cause is required, it seems that DOD would need specific evidence before deciding which messages to intercept. Thus, for example, DOD must have some information that a certain person might be a terrorist, or that a certain phone line might be used by a terrorist, before it can capture the communications. This means that the NSA cannot intercept communications for which it has no such evidence. This would be the case even if the President were to require that there be reasonable grounds to believe that the communications involve the relevant foreign country or terrorists. This has the effect of excluding communications for which DOD has no reason to suspect contain terrorist communications or communications with the foreign country, meaning that most innocent communications will not be

⁴Another factor examined by the Court was effectiveness of the warrantless search. The Court has cautioned that searches not be random and discretionless because of a lack of empirical evidence that the means would promote the government's interest. It should be made clear, however, that the standard employed by the Court has been low. In the roadblock context, for example, the Court has found reasonable roadblocks for drunk drivers that detained only 1.6 percent of all drivers stopped, and checkpoints for illegal aliens that detained only 0.12 percent of all vehicles detained.

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

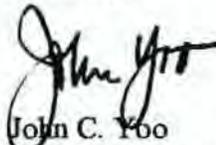
intercepted.

Further, limiting the search parameters to international communications could further alleviate any intrusion into individual privacy interests. As our discussion of the border search exception in Part III made clear, the government has the constitutional authority to search anything that crosses the Nation's borders without violating the Fourth Amendment. To be sure, there is substantial doubt about whether this power could apply to searches involving the content of the communications. Nonetheless, *United States v. Ramsey*, 431 U.S. 606 (1977) (warrantless search of incoming international mail does not violate Fourth Amendment), suggests strongly that individuals have reduced privacy interests when they or their possessions and letters cross the borders of the United States. If individuals have reduced privacy interests in international mail, as *Ramsey* held, then it seems logical to assume that they also have a reduced privacy interest in international electronic communications as well. As *Ramsey* held, the method by which an item entered the country is irrelevant for Fourth Amendment purposes.

Just to be clear in conclusion. We are not claiming that the government has an unrestricted right to examine the contents of all international letters and other forms of communication. Rather, we are only suggesting that an individual has a reduced privacy interest in international communications. Therefore, in applying the balancing test called for by the Fourth Amendment's reasonableness analysis, we face a situation here where the government's interest on one side – that of protecting the Nation from direct attack – is the highest known to the Constitution. On the other side of the scale, the intrusion into individual privacy interests is greatly reduced due to the international nature of the communications. Thus, we believe there to be substantial justification for a warrantless electronic surveillance program, undertaken in response to the September 11, 2001 attacks, that would be reasonable under the Fourth Amendment.

I would welcome the opportunity to discuss these issues in more detail. Please contact me, at 202-514-2069, or john.c.yoo@usdoj.gov, if you have any further questions.

Sincerely,



John C. Yoo
Deputy Assistant Attorney General

AUTHORITY FOR WARRANTLESS NATIONAL SECURITY SEARCHES

Presidents have long asserted the constitutional authority to order searches, even without judicial warrants, where necessary to protect the national security against foreign powers and their agents. The courts have repeatedly upheld the exercise of this authority.

A memorandum from President Franklin D. Roosevelt to Attorney General Robert H. Jackson, dated May 21, 1940, authorized the use of wiretaps in matters “involving the defense of the nation.” See *United States v. United States District Court for the Eastern District of Michigan*, 407 U.S. 297, 311 n.10 (1972) (“*Keith*”). The President directed the Attorney General “to secure information by listening devices [directed at] the conversation or other communications of persons suspected of subversive activities against the government of the United States, including suspected spies,” while asking the Attorney General “to limit these investigations so conducted to a minimum and to limit them insofar as possible as to aliens.” See *Electronic Surveillance Within the United States for Foreign Intelligence Purposes: Hearings Before the Subcomm. on Intelligence and the Rights of Americans of the Select Comm. on Intelligence, 94th Cong., 2d Sess. 24 (1976)* (statement of Attorney General Edward H. Levi) (“Levi Statement”). President Roosevelt issued the memorandum after the House of Representatives passed a joint resolution to sanction wiretapping by the FBI for national security purposes, but the Senate failed to act. See Americo R. Cinquegrana, *The Walls and Wires Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. Pa. L. Rev. 793, 797-98 (1989).

By a letter dated July 17, 1946, Attorney General Tom C. Clark reminded President Truman of the 1940 directive, which had been followed by Attorneys General Jackson and Francis Biddle. At Attorney General Clark’s request, the President approved the continuation of the authority, see Levi Statement at 24, and even broadened it to reach “internal security cases.” *Keith*, 407 U.S. at 311 and n.10. In the Eisenhower Administration, Attorney General Herbert Brownell, as the Supreme Court noted in *Keith*, advocated the use electronic surveillance both in internal and international security matters. 407 U.S. at 311.

In 1965, President Johnson announced a policy under which warrantless wiretaps would be limited to national security matters. Levi Statement at 26. Attorney General Katzenbach then wrote that he saw “no need to curtail any such activities in the national security field.” *Id.* Attorney General Richardson stated in 1973 that, to approve a warrantless surveillance, he would need to be convinced that it was necessary “(1) to protect the nation against actual or potential attack or other hostile acts of a foreign power, (2) to obtain foreign intelligence information deemed essential to the security of the United States, or (3) to protect national security information against foreign intelligence activities.” *Id.* at 27. When Attorney General Levi testified in 1976, he gave a similar list, adding that a warrantless surveillance could also be used “to obtain information certified as necessary for the conduct of foreign

affairs matters important to the national security of the United States.” *Id.*

Warrantless electronic surveillance of agents of foreign powers thus continued until the passage in 1978 of the Foreign Intelligence Surveillance Act, 18 U.S.C. §§ 1801-29. Although the Supreme Court never ruled on the legality of warrantless searches as to agents of foreign powers, *see Keith*, 407 U.S. at 321-22 (requiring a warrant in domestic security cases but reserving issue where a foreign power or its agents were involved), the courts of appeals repeatedly sustained the lawfulness of such searches. *United States v. Truong Dinh Hung*, 629 F.2d 908, 914 (4th Cir. 1980); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977); *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973); *United States v. Butenko*, 494 F.2d 593, 606 (3d Cir. 1974); *United States v. Clay*, 430 F.2d 165 (5th Cir. 1970), *rev'd on other grounds*, 403 U.S. 698 (1971); *but see Zweibon v. Mitchell*, 516 F.2d 594, 651 (D.C. Cir. 1975) (dictum in plurality opinion). The Fourth Circuit held, for example, that “because of the need of the executive branch for flexibility, its practical experience, and its constitutional competence, the courts should not require the executive to secure a warrant each time it conducts foreign intelligence surveillance.” *Truong*, 629 F.2d at 914. As the court elaborated, “attempts to counter foreign threats to the national security require the utmost stealth, speed, and secrecy,” and a “warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, in some cases delay executive response to foreign intelligence threats, and increase the chance of leaks regarding sensitive executive operations.” *Id.* at 913 (citations and footnote omitted). Furthermore, “the executive possesses unparalleled expertise to make the decisions whether to conduct foreign intelligence surveillance.” *Id.* (citations omitted). And “[p]erhaps most crucially, the executive branch not only has superior expertise in the area of foreign intelligence, it is also constitutionally designated as the pre-eminent authority in foreign affairs.” *Id.* at 914 (citations omitted). In this pre-statutory context, two courts of appeals, the Fourth Circuit in *Truong* (*id.* at 915) and the Third Circuit in *Butenko* (494 F.2d at 606), would have limited the authority to instances where the primary purpose of the search was to obtain foreign intelligence.”

The passage of FISA created an effective means for issuance of judicial orders for electronic surveillance in national security matters. Congress, however, had not given the Foreign Intelligence Surveillance Court the power to issue orders for physical searches. After nevertheless granting orders in three instances during the Carter Administration, the court ruled early in the Reagan Administration, as the Justice Department then argued, that it lacked jurisdiction to approve physical searches. *See S. Rep. 103-296*, at 36-37 (1994). Thus, physical searches after the ruling had to be approved by the Attorney General without a judicial warrant. *Id.* at 37. In 1994, after the use of warrantless physical searches in the Aldrich Ames case, Congress concluded that “from the standpoint of protecting the constitutional rights of Americans, from the standpoint of bringing greater legal certainty to this area, from the standpoint of avoiding problems with future espionage prosecutions, and from the standpoint of protecting federal officers and employees from potential civil liability,” *id.*, FISA should be amended to cover physical searches. *Id.* at 40.

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

AMERICAN CIVIL LIBERTIES UNION,
and AMERICAN CIVIL LIBERTIES
UNION FOUNDATION,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY,
CENTRAL INTELLIGENCE AGENCY,
DEPARTMENT OF DEFENSE,
DEPARTMENT OF JUSTICE, and
DEPARTMENT OF STATE,

Defendants.

No. 13 Civ. 9198 (AT)

DECLARATION OF JONATHAN MANES

I, Jonathan Manes, pursuant to 28 U.S.C. § 1746, hereby declare:

1. I am a supervising attorney at the Media Freedom and Information Access Clinic (“MFIA Clinic”), which represents Plaintiffs American Civil Liberties Union and American Civil Liberties Union Foundation (“ACLU”) in this action concerning Freedom of Information Act (“FOIA”) requests that seek records from the National Security Agency (“NSA”), Central Intelligence Agency (“CIA”), Department of Defense (“DOD”), Department of Justice (“DOJ”), and Department of State (“State”) regarding their EO 12333 implementing regulations, formal training materials, official authorizations of surveillance programs, implementing regulations, and formal legal opinions addressing surveillance under EO 12333 that implicates U.S. persons.

2. I am an attorney licensed to practice law in the State of New York and the State of New Jersey. I am admitted to the bar of this Court.

JA417

3. I submit this declaration in support of the ACLU's cross-motion for partial summary judgment and in opposition to Defendants' motion for partial summary judgment.

4. Attached hereto as **Exhibit A** is a true and correct copy of Plaintiffs' Index of Contested Documents.

5. Attached hereto as **Exhibit B** is a true and correct copy of John C. Yoo, Deputy Assistant Attorney General, Office of Legal Counsel, Memorandum for the Attorney General (Nov. 2, 2001) ("OLC 8").

6. Attached hereto as **Exhibit C** is a true and correct copy of Letter from John C. Yoo, Deputy Assistant Attorney General, Office of Legal Counsel, to Judge Colleen Kollar-Kotelly, U.S. District Court for the District of Columbia (May 17, 2002) ("OLC 9").

7. Attached hereto as **Exhibit D** is a true and correct copy of Office of Legal Counsel, Memorandum for the Attorney General, *Re: Review of the Legality of the STELLAR WIND Program* (May 6, 2004) ("OLC 10").

8. Attached hereto as **Exhibit E** is a true and correct copy of excerpts from Department of Justice, Office of the Inspector General, *A Review of the Department of Justice's Involvement with the President's Surveillance Program* (July 2009) ("OIG Report"), which is included in Offices of Inspectors General of the Department of Defense, Office of Director of National Intelligence, Department of Justice, Central Intelligence Agency, National Security Agency, *Report on the President's Surveillance Program* (July 10, 2009).

9. Attached hereto as **Exhibit F** is a true and correct copy of Office of General Counsel, Memorandum for the Deputy Chief of Staff, *Sharing of 'Raw Sigint' Through Database Access* ("NSA 28").

10. Attached hereto as **Exhibit G** is a true and correct copy of Kenneth L. Wainstein, Assistant Attorney General, National Security Division, *Proposed Amendment to Department of Defense Procedures to Permit the National Security Agency to Conduct Analysis of Communications Metadata Associated with Persons in the United States* (Nov. 20, 2007) (“Wainstein Memo”), obtained via *Justice Department and NSA Memos Proposing Broader Powers for NSA to Collect Data*, Guardian, June 27, 2013, <http://bit.ly/1XJcRmy>.

11. Attached hereto as **Exhibit H** is a true and correct copy of Assistant General Counsel, Defense Intelligence Agency, “DoD Humint Legal Workshop: Fundamentals of Humint Targeting” (“DIA V-4”).

12. Attached hereto as **Exhibit I** is a true and correct copy of *Fiscal Year 2012 National Clandestine Service Report to HPSCI and SSCI on Executive Order 12333* (2012) (“CIA 12”).

13. Attached hereto as **Exhibit J** is a true and correct copy of National Security Agency, Memorandum for the Chairman, Intelligence Oversight Board, *Report to the Intelligence Oversight Board on NSA Activities—Information Memorandum* (Mar. 4, 2013) (“NSA 79”).

14. Attached hereto as **Exhibit K** is a true and correct copy of Inspector General, Central Intelligence Agency, *Compliance with Executive Order 12,333: The Use of [Redacted] Collection [Redacted] from 1995-2000* (Aug. 7, 2002) (“CIA 10”).

15. Attached hereto as **Exhibit L** is a true and correct copy of Memorandum for the Secretary of Defense, *Classified Annex to Department of Defense Procedures Under Executive Order 12,333—Action Memorandum* (Apr. 4, 1988) (“NSD 94-125”).

16. Attached hereto as **Exhibit M** is a true and correct copy of National Security Agency, Procedures Governing NSA/CSS Activities That Affect U.S. Persons (May 29, 2009), which includes the *Classified Annex to Department of Defense Procedures Under Executive Order 12,333*.

17. Attached hereto as **Exhibit N** is a true and correct copy of Central Intelligence Agency, "AR 2-2 Collection Rules" (January 2014). ("CIA 11").

18. Attached hereto as **Exhibit O** is a true and correct copy of Central Intelligence Agency, *AR 2-2: Law and Policy Governing the Conduct of Intelligence Activities* (Dec. 23, 1987) ("CIA 1").

19. Attached hereto as **Exhibit P** is a true and correct copy of *Supplemental Guidelines for Collection, Retention, and Dissemination of Foreign Intelligence* (Nov. 29, 2006) ("NSD 202-207").

20. Attached hereto as **Exhibit Q** is a true and correct copy of *AR 2-2E Annex E: Memorandum of Understanding Concerning Overseas and Domestic Activities of the Central Intelligence Agency and Domestic Activities of the Central Intelligence Agency and the Federal Bureau of Investigation* (Dec. 23, 1987) ("CIA 4").

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 20th day of April, 2016, at New Haven, Connecticut.



Jonathan Manes

EXHIBIT E

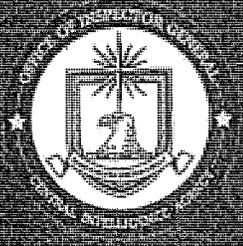
JA421

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~ 37.3

(U) REPORT ON THE
PRESIDENT'S SURVEILLANCE PROGRAM

VOLUME I

10 JULY 2009



PREPARED BY THE
OFFICES OF INSPECTORS GENERAL
OF THE
DEPARTMENT OF DEFENSE
DEPARTMENT OF JUSTICE
CENTRAL INTELLIGENCE AGENCY
NATIONAL SECURITY AGENCY
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Special Warning

The report contains compartmented, classified material and no secondary distribution may be made without prior consent of the participating Inspectors General. Improper disclosure of this report may result in criminal, civil, or administrative penalties.

REPORT NO. 2009-0013-A

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~
JA422

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

U.S. Department of Justice
Office of the Inspector General

A Review of the Department of Justice's Involvement with the President's Surveillance Program (U)



Department of Justice
Office of the Inspector General
Oversight and Review Division
July 2009

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

Derived From: NSA/CSS M 1-52, 2-400
NSA/CSS M 1-52, 12-48

Dated: 20070108

Declassify On: 20340713

JA423

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

TABLE OF CONTENTS

CHAPTER ONE: INTRODUCTION (U) 1

I. Methodology of OIG Review (U) 3

II. Organization of this Report (U) 5

CHAPTER TWO: LEGAL AUTHORITIES (U) 7

I. Constitutional, Statutory, and Executive Order Authorities (U) 7

A. Article II, Section 2 of the Constitution (U) 7

B. The Fourth Amendment (U)..... 7

C. The Foreign Intelligence Surveillance Act (FISA) (U)..... 8

 1. Overview of FISA (U) 8

 2. FISA Applications and Orders (U) 10

 3. FISA Court (U)..... 11

D. Authorization for Use of Military Force (U)..... 12

E. Executive Order 12333 (U)..... 13

II. Presidential Authorizations (U) 14

A. Types of Collection Authorized ~~(S//NF)~~..... 15

B. Findings and Primary Authorities (U) 16

C. The Reauthorization Process (U)..... 16

D. Approval “as to form and legality” (U) 17

CHAPTER THREE: INCEPTION AND EARLY OPERATION OF STELLAR WIND (SEPTEMBER 2001 THROUGH APRIL 2003) ~~(S//NF)~~..... 19

I. Inception of the Stellar Wind Program (U//~~FOUO~~)..... 19

A. The National Security Agency (U) 19

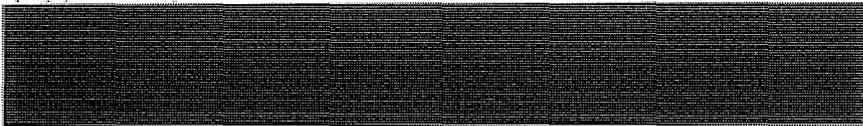
B. Implementation of the Program (September 2001 through November 2001) ~~(S//NF)~~..... 20

 1. Pre-Stellar Wind Office of Legal Counsel Legal Memoranda (U)..... 23

 2. Presidential Authorization of October 4, 2001 ~~(TS//SI//NF)~~..... 28

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

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

- C. Presidential Authorization is Revised and the Office of Legal Counsel Issues Legal Memoranda in Support of the Program (November 2001 through January 2002)
 - ~~(TS//STLW//SI//OC/NF)~~..... 31
 - 1. Presidential Authorization of November 2, 2001
 - ~~(TS//SI//NF)~~..... 31
 - 2. Yoo Drafts Office of Legal Counsel Memorandum Addressing Legality of Stellar Wind
 - ~~(TS//STLW//SI//OC/NF)~~..... 33
 - 3. Additional Presidential Authorizations (U) 38
 - 4. Subsequent Yoo Opinions (U) 39
 - 5. Yoo's Communications with the White House (U)..... 40
 - 6. Gonzales's View of the Department's Role in Authorizing the Stellar Wind Program ~~(S//NF)~~..... 41
- II. NSA's Implementation of the Stellar Wind Program (U//~~FOUO~~)..... 42
 - A. Implementation of Stellar Wind (U//~~FOUO~~) 42
 - 1. Basket 1 – Telephone and E-Mail Content Collection
 - ~~(TS//STLW//SI//OC/NF)~~..... 44
 - 2. Basket 2 – Telephony Meta Data Collection
 - ~~(TS//STLW//SI//OC/NF)~~..... 48
 - 3. Basket 3 – E-Mail Meta Data Collection
 - ~~(TS//STLW//SI//OC/NF)~~..... 51
 - B. NSA Process for Analyzing Information Collected Under Stellar Wind ~~(S//NF)~~ 52
 - 1. Basket 1: Content tasking, Analysis, and Dissemination ~~(TS//STLW//SI//OC/NF)~~..... 52
 - 2. Baskets 2 and 3: Telephony and E-Mail Meta Data Queries, Analysis, and Dissemination
 - ~~(TS//STLW//SI//OC/NF)~~..... 54
- III. FBI's Early Participation in the Stellar Wind Program ~~(S//NF)~~..... 58
 - A. FBI Director First Informed of Stellar Wind Program (U//~~FOUO~~)..... 59
 - B.  59
 - C. FBI Begins to Receive and Disseminate Stellar Wind "Tippers" ~~(S//NF)~~..... 63
 - 1. FBI Initiates  (S//NF) 63
 - 2. FBI Field Offices' Response to  Leads ~~(S//NF)~~..... 67

b1, b3, b7E

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

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

3.	FBI's Efforts to Track Stellar Wind Tippers and Update Executive Management on Status of [REDACTED] Leads (S//NF).....	69	b1, b3, b7E
IV.	Justice Department Office of Intelligence Policy and Review's (OIPR) and FISA Court's Early Role in Stellar Wind (TS//STLW//SI//OC/NF).....	70	
A.	Overview of OIPR (U).....	71	
B.	OIPR Counsel Learns of Stellar Wind Program (U//FOUO)....	71	
C.	FISA Court is Informed of Stellar Wind (TS//SI//NF).....	74	
D.	OIPR Implements "Scrubbing" Procedures for Stellar Wind Information in International Terrorism FISA Applications (TS//STLW//SI//OC/NF)	78	
1.	Initial Scrubbing Procedures (TS//SI//NF).....	79	
2.	Complications with Scrubbing Procedures (TS//SI//NF).....	81	
E.	Judge Kollar-Kotelly Succeeds Judge Lamberth as FISA Court Presiding Judge (U).....	83	
1.	Judge Kollar-Kotelly Modifies OIPR Scrubbing Procedures (TS//SI//NF)	83	
2.	OIPR implements Judge Kollar-Kotelly's Scrubbing Procedure (TS//SI//NF).....	85	
V.	FBI Initiates Measures to Improve the Management of Stellar Wind Information (S//NF).....	88	
A.	CAU Acting Unit Chief Evaluates FBI Response to Stellar Wind (S//NF).....	89	
B.	FBI Increases Cooperation with NSA and Initiates [REDACTED] Project to Manage Stellar Wind Information (TS//STLW//SI//OC/NF)	90	b1, b3, b7E
C.	FBI Assigns CAU Personnel to NSA on Full-Time Basis (S//NF)	93	
VI.	OIG Analysis (U).....	94	
CHAPTER FOUR: LEGAL REASSESSMENT OF STELLAR WIND (MAY 2003 THROUGH MAY 2004) (TS//SI//NF).....		99	
I.	Justice Department Reassesses Legality of Stellar Wind Program (TS//SI//NF).....	99	
A.	Overview of Office of Legal Counsel (U).....	99	

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

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

B.	Personnel Changes within Office of Legal Counsel (U)	100
1.	Yoo's Role in the Program (October 2001 through May 2003) (U)	100
2.	Philbin Replaces Yoo (U).....	103
3.	Initial Concerns with Yoo's Analysis (U)	104
4.	Problems with [REDACTED] (TS//STLW//SI//OC/NF).....	106
5.	Other Collection Concerns (S//NF).....	108
6.	Decision to Draft New OLC Memorandum (U).....	108
C.	Reassessment of Legal Rationale for the Program (TS//SI//NF)	109
1.	Goldsmith Becomes OLC Assistant Attorney General (U).....	109
2.	NSA Denied Access to OLC Memoranda (U//FOUO) ..	111
3.	Goldsmith Joins Effort to Reassess Legal Basis for the Program (TS//SI//NF)	112
4.	AUMF Becomes the Primary Legal Rationale Supporting [REDACTED] of the Stellar Wind Program (TS//STLW//SI//OC/NF).....	113
5.	Office of Legal Counsel Raises its Reassessment of the Stellar Wind Program (December 2003 through January 2004) (TS//SI//NF).....	115
6.	Deputy Attorney General Comey is Read into the Program (U).....	118
D.	Office of Legal Counsel Presents its Conclusions to the White House (U)	119
1.	March 4, 2004: Comey Meets with Ashcroft to Discuss Problems with the Program (U).....	120
2.	March 5, 2004: Comey Determines Ashcroft is "Absent or Disabled" (U).....	121
3.	March 5, 2004: Goldsmith and Philbin Seek Clarification from White House on Presidential Authorizations (U)	122
4.	March 6 to 8, 2004: The Department Concludes That Yoo's Legal Memoranda Did Not Cover the Program (U).....	124
5.	March 9, 2004: White House Seeks to Persuade Department and FBI to Support Continuation of the Program (S//NF).....	126
6.	Conflict Ensues between Department and White House (U).....	129
II.	White House Continues Program without Justice Department's Certification (TS//SI//NF).....	130

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

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

A. White House Counsel Gonzales Certifies March 11, 2004, Presidential Authorization ~~(TS//SI//NF)~~..... 131

1. March 10, 2004: Office of Legal Counsel Presses for Solicitor General to be Read into Program (U) 131
2. March 10, 2004: Congressional Leaders Briefed on Situation (U)..... 131
3. March 10, 2004: Hospital Visit (U)..... 134
4. March 10, 2004: Olson is Read into the Program (U). 140
5. March 11, 2004: Goldsmith Proposes Compromise Solution (U)..... 141
6. March 11, 2004: White House Asserts that Comey's Status as Acting Attorney General was Unclear (U) 142
7. March 11, 2004: Gonzales Certifies Presidential Authorization as to Form and Legality ~~(TS//SI//NF)~~: 144

B. Department and FBI Officials React to Issuance of March 11, 2004, Authorization ~~(TS//SI//NF)~~..... 148

1. Initial Responses of Department and FBI Officials (U) 149
2. Department and FBI Officials Consider Resigning (U) 152
3. Comey and Mueller Meet with President Bush (U)..... 155
4. Comey Directs Continued Cooperation with NSA (U).. 157
5. Department Conducts Additional Legal Analysis (U)... 158
6. Comey Determines that Ashcroft Remains "Absent or Disabled" (U) 163
7. Judge Kollar-Kotelly Briefed on Lack of Attorney General Certification (U) 164
8. Comey and Gonzales Exchange Documents Asserting Conflicting Positions (U) 164

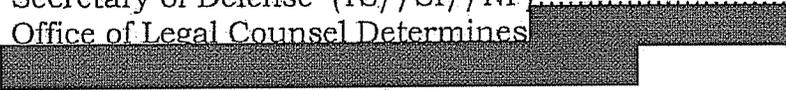
C. White House Agrees to [REDACTED] ~~(TS//STLW//SI//OC/NF)~~ 168

1. March 19, 2004, Modification (U)..... 168
2. [REDACTED] 172
3. [REDACTED] 173
4. [REDACTED] 175
5. Judge Kollar-Kotelly is Presented with the OLC Legal Analysis Regarding [REDACTED] ~~(TS//STLW//SI//OC/NF)~~..... 175
6. April 2, 2004, Modification (U) 178

b1, b3, b7E

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

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

7.	 Standard is Conveyed to the FBI (TS//SI//NF)	180
8.	Office of Legal Counsel Assesses NSA's Compliance with New Collection Standards (TS//SI//NF)	180
9.	May 5, 2004, Presidential Authorization (TS//SI//NF)	181
10.	May 6, 2004, OLC Memorandum (TS//SI//NF)	182
III.	OIG Analysis (U)	186
A.	Department's Access to and Legal Review of Stellar Wind Program Through May 2004 (TS//SI//NF)	186
B.	The Hospital Visit (U).....	197
C.	Recertification of the Presidential Authorization and Modification of the Program (U).....	199
 CHAPTER FIVE: STELLAR WIND PROGRAM'S TRANSITION TO FISA AUTHORITY (JUNE 2004 THROUGH AUGUST 2007)		
I.	E-Mail Meta Data Collection Under FISA (TS//SI//NF)	203
A.	Application and FISA Court Order (U).....	203
1.	Decision to Seek a Pen Register and Trap and Trace (PR/TT) Order from the FISA Court (TS//SI//NF)	203
2.	Briefing for Judge Kollar-Kotelly (U)	205
3.	The PR/TT Application (TS//SI//NF)	205
4.	Judge Kollar-Kotelly Raises Questions about PR/TT Application (TS//SI//NF)	212
5.	FISA Court Order (U).....	213
B.	President Orders Limited Use  (TS//STLW//SI//OC/NF)	217
1.	The President's August 9, 2004, Memorandum to the Secretary of Defense (TS//SI//NF)	217
2.	Office of Legal Counsel Determines  (TS//STLW//SI//OC/NF)	218
C.	Non-Compliance with PR/TT Order (TS//SI//NF)	219
1.	Filtering Violations (TS//SI//NF)	219
2.	FISA Court Renews PR/TT Order (TS//SI//NF)	221
3.		222
D.	Subsequent PR/TT Applications and Orders (TS//SI//NF)	224
II.	Telephony Meta Data Collection Under FISA (TS//SI//NF)	225

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

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

- A. Decision to Seek Order Compelling Production of Call detail records (TS//SI//NF)..... 226
- B. Summary of Department’s Application and Related FISA Court Order (S/NF)..... 228
- C. Non-Compliance with Section 215 Orders (TS//SI//NF) 232
- III. Content Collection under FISA (TS//SI//NF) 237
 - A. Decision to Seek Content Order (TS//SI//NF) 237
 - B. Summary of Department’s December 13, 2006, Content Application (TS//SI//NF) 239
 - C. Judge Howard Grants Application in Part (TS//SI//NF) 245
 - D. Domestic Selectors Application and Order (TS//SI//NF)..... 248
 - E. Last Stellar Wind Presidential Authorization Expires (TS//SI//NF)..... 250
 - F. First Domestic and Foreign Selectors FISA Renewal Applications (TS//SI//NF)..... 251
 - G. Revised Renewal Application for Foreign Selectors and Order (TS//SI//NF)..... 255
- IV. The Protect America Act and the FISA Amendments Act of 2008 (U)..... 259
 - A. The Protect America Act (U) 260
 - B. The FISA Amendments Act of 2008 (U)..... 264
- V. OIG Analysis (U)..... 267
- CHAPTER SIX: [REDACTED] (S//NF) 271
 - I. [REDACTED] Process (S//NF)..... 272
 - II. FBI’s Decision to Issue National Security Letters under [REDACTED] to Obtain Telephone Subscriber Information (S//NF) 277
 - III. [REDACTED] and Scrubbing Process (TS//SI//NF)..... 284
 - IV. Impact of Stellar Wind Information on FBI Counterterrorism Efforts (S//NF)..... 291
 - A. Stellar Wind/[REDACTED] Statistics (TS//STLW//SI//OC/NF) 291
 - B. FBI Field Office Investigations of [REDACTED] Tippers (S//NF) 296

b1, b3, b7E

b1, b3, b7E

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

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

C.	FBI Statistical Surveys of ██████████ Meta Data Tippers (TS//STLW//SI//OC/NF)	300	b1, b3, b7E
1.	Early 2006 Survey of ██████████ Telephony and E-Mail Meta Data Tippers (TS//STLW//SI//OC/NF)	301	b1, b3, b7E
2.	January 2006 Survey of ██████████ E-Mail Meta Data Tippers (TS//STLW//SI//OC/NF)	304	
D.	FBI Judgmental Assessments of Stellar Wind Information (S//NF)	305	
E.	Examples of FBI Counterterrorism Cases Involving Stellar Wind Information (S//NF)	310	
1.	██████████	311	
2.	██████████	313	b1, b3, b6, b7C, b7E
3.	██████████	315	
4.	██████████	318	
5.	██████████	322	
V.	OIG Analysis (U)	325	

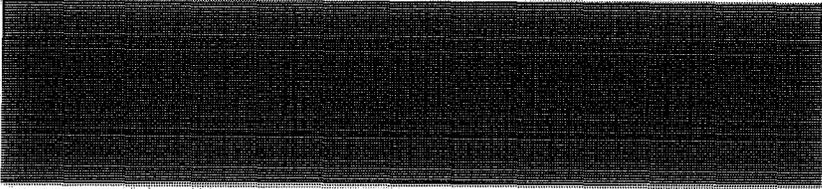
CHAPTER SEVEN: DISCOVERY ISSUES RELATED TO STELLAR WIND
INFORMATION (TS//SI//NF)..... 333

I.	Relevant Law (U)	333	
II.	Cases Raise Questions about Government's Compliance with Discovery Obligations (U)	335	
A.	██████████	335	b1, b3, b6, b7C, b7E
B.	██████████	336	
III.	Criminal Division Examines Discovery Issues (U)	340	
A.	The "Informal Process" for Treating Discovery Issues in International Terrorism Cases (U)	341	
B.	██████████ Memorandum Analyzing Discovery Issues Raised by the Stellar Wind Program (TS//STLW//SI//OC/NF).....	342	
C.	Office of Legal Counsel and Discovery Issue (U)	346	
IV.	Use of the Classified Information Procedures Act (CIPA) to Respond to Discovery Requests (U)	347	
A.	Overview of CIPA (U)	348	
B.	Use of CIPA in International Terrorism Prosecutions Alleged to Involve Stellar Wind-Derived Information (TS//STLW//SI//OC/NF)	348	

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

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

C. Government Arguments in Specific Cases (U) 351

 351 b1, b3,
..... 353 b6,
..... 354 b7C,
..... 355 b7E

V. OIG ANALYSIS (U) 357

CHAPTER EIGHT: PUBLIC STATEMENTS ABOUT THE SURVEILLANCE PROGRAM (U) 361

I. Summary of the Dispute about the Program (U) 361

II. The New York Times Articles and President Bush’s Confirmation Regarding NSA Activities (U) 363

III. Other Administration Statements (U) 365

IV. Testimony and Other Statements (U) 366

A. Gonzales’s February 6, 2006, Senate Judiciary Committee Testimony (U) 367

B. Comey’s May 15, 2007, Senate Judiciary Committee Testimony (U) 370

C. Gonzales’s June 5, 2007, Press Conference (U) 371

D. Gonzales’s July 24, 2007, Senate Judiciary Committee Testimony (U) 371

E. FBI Director Mueller’s July 26, 2007, House Committee on the Judiciary Testimony (U) 376

F. Gonzales’s Follow-up Letter to the Senate Judiciary Committee (U) 377

V. OIG Analysis (U) 378

CHAPTER NINE: CONCLUSIONS (U) 387

I. Operation of the Program (U//~~FOUO~~) 388

II. Office of Legal Counsel’s Analysis of the Stellar Wind Program ~~(TS//SI//NF)~~ 389

III. Hospital Visit and White House Recertification of the Program (U) 394

IV. Transition of Program to FISA Authority ~~(TS//STLW//SI//OC/NF)~~ 396

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

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

V.	Impact of Stellar Wind Information on FBI Counterterrorism Efforts (S//NF)	397
VI.	Discovery and "Scrubbing" Issues (TS//SI//NF).....	402
VII.	Gonzales's Statements (U).....	404
VIII.	Conclusion (U).....	406

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

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

electronic surveillance, as defined under FISA, must be conducted in accordance with FISA.¹⁶ (U)

Executive Order 12333 prohibits the collection of foreign intelligence information by "authorized [agencies] of the Intelligence Community . . . for the purpose of acquiring information concerning the domestic activities of United States persons." Id. at 2.3(b). (U)

However, in authorizing the Stellar Wind program, [REDACTED]

[REDACTED] As discussed previously, the legal rationale advanced for this exemption was that the Authorization for Use of Military Force and the President's Commander-in-Chief powers gave the President the authority to collect such information, notwithstanding the FISA statute. ~~(TS//STLW//SI//OC/NF)~~

II. Presidential Authorizations (U)

The Stellar Wind program was first authorized by the President on October 4, 2001, and periodically reauthorized by the President through a series of documents issued to the Secretary of Defense entitled "Presidential Authorization for Specified Electronic Surveillance Activities During a Limited Period to Detect and Prevent Acts of Terrorism Within the United States" (Presidential Authorization or Authorization). A total of 43 Presidential Authorizations, not including modifications and related presidential memoranda, were issued over the duration of the program from October 2001 through February 2007.¹⁷ Each Authorization directed the

¹⁶ Prior to September 11, 2001, Executive Order 12333 and FISA were generally viewed as the principal governing authorities for conducting electronic surveillance. For example, in 2000 the NSA reported to Congress that

(U) The applicable legal standards for the collection, retention, or dissemination of information concerning U.S. persons reflect a careful balancing between the needs of the government for such intelligence and the protection of the rights of U.S. persons, consistent with the reasonableness standard of the Fourth Amendment, as determined by factual circumstances.

(U) In the Foreign Intelligence Surveillance Act (FISA) and Executive Order (E.O.) 12333, Congress and the Executive have codified this balancing. (Citations omitted.)

NSA Report to Congress, *Legal Standards for the Intelligence Community in Conducting Electronic Surveillance* (2000). (U)

¹⁷ The Presidential Authorizations were issued on the following dates: October 4, 2001; November 2, 2001; November 30, 2001; January 9, 2002; March 14, 2002; April 18, 2002; May 22, 2002; June 24, 2002; July 30, 2002; September 10, 2002; October 15, 2002; November 18, 2002; January 8, 2003; February 7, 2003; March 17, 2003; April 22, 2003. (Cont'd.)

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

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

Secretary of Defense to “use the capabilities of the Department of Defense, including but not limited to the signals intelligence capabilities of the National Security Agency, to collect foreign intelligence by electronic surveillance,” provided the surveillance met certain criteria. The specific criteria are described in detail in Chapters Three and Four of this report. ~~(TS//STLW//SI//OC/NF)~~

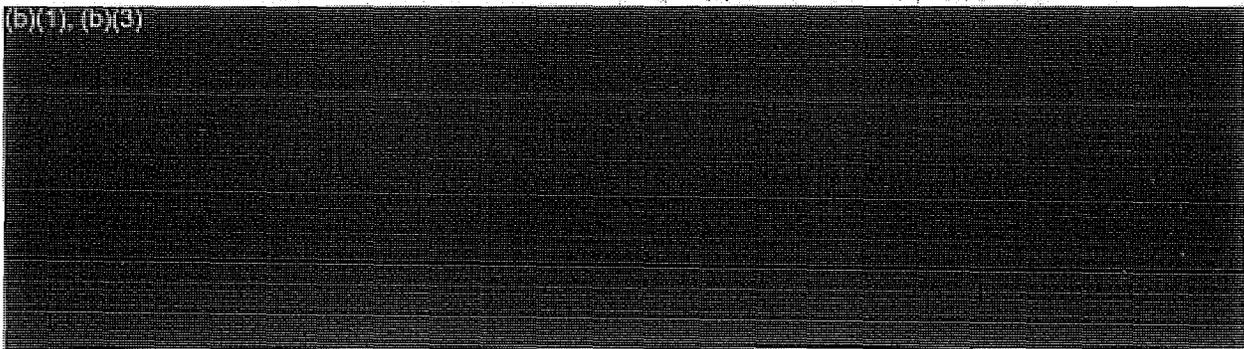
A. Types of Collection Authorized ~~(S//NF)~~

The scope of collection permitted under the Presidential Authorizations varied over time, but generally involved intercepting the content of certain telephone calls and e-mails, and the collection of bulk telephone and e-mail meta data. The term “meta data” has been described as “information about information.” As used in the Stellar Wind program, for telephone calls, meta data generally refers to “dialing-type information” (the originating and terminating telephone numbers, and the date, time, and duration of the call), but not the content of the call. For e-mails, meta data generally refers to the “to,” “from,” “cc,” “bcc,” and “sent” lines of an e-mail, but not the “subject” line or content. ~~(TS//STLW//SI//OC/NF)~~

The information collected through the Stellar Wind program fell into three categories, often referred to as “baskets”:

- Basket 1 (content of telephone and e-mail communications);
- Basket 2 (telephony meta data); and
- Basket 3 (e-mail meta data). ~~(TS//STLW//SI//OC/NF)~~

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



2003; June 11, 2003; July 14, 2003; September 10, 2003; October 15, 2003; December 9, 2003; January 14, 2004; March 11, 2004; May 5, 2004; June 23, 2004; August 9, 2004; September 17, 2004; November 17, 2004; January 11, 2005; March 1, 2005; April 19, 2005; June 14, 2005; July 26, 2005; September 10, 2005; October 26, 2005; December 13, 2005; January 27, 2006; March 21, 2006; May 16, 2006; July 6, 2006; September 6, 2006; October 24, 2006; and December 8, 2006. The last Presidential Authorization expired February 1, 2007. There were also two modifications of a Presidential Authorization and one Presidential memorandum to the Secretary of Defense issued in connection with the Stellar Wind program. ~~(TS//STLW//SI//OC/NF)~~

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

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

value. As the period for each Presidential Authorization drew to a close, the Director of Central Intelligence (DCI), and as of June 3, 2005, the Director of National Intelligence (DNI) prepared a threat assessment memorandum for the President describing potential terrorist threats to the United States and outlining intelligence gathered through the Stellar Wind program and other means during the previous Authorization period. The DCI (and later the DNI) and the Secretary of Defense reviewed these memoranda and signed a recommendation that the program be reauthorized.

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

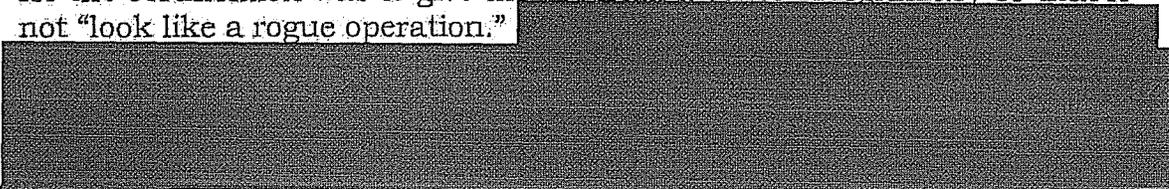
Each recommendation was then reviewed by the OLC to assess whether, based on the threat assessment and information gathered from other sources, there was "a sufficient factual basis demonstrating a threat of terrorist attacks in the United States for it to continue to be reasonable under the standards of the Fourth Amendment for the President to [continue] to authorize the warrantless searches involved" in the program. The OLC then advised the Attorney General whether the constitutional standard of reasonableness had been met and whether the Presidential Authorization could be certified "as to form and legality."

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

D. Approval "as to form and legality" (U)

As noted above, the Presidential Authorizations were "[a]pproved as to form and legality" by the Attorney General or other senior Department official, typically after the review and concurrence of the OLC. The lone exception to this practice was the March 11, 2004, Authorization which we discuss in Chapter Four. ~~(TS//SI//NF)~~

However, there was no legal requirement that the Authorizations be certified by the Attorney General or other Department official. Former senior Department official Patrick Philbin told us he thought one purpose for the certification was to give the program a sense of legitimacy so that it not "look like a rogue operation."

 Bradbury told us that the Justice Department certifications served as official confirmation that the Department had determined that the activities carried out under the program were lawful.

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

Former Attorney General Gonzales told us that certification of the program as to form and legality was not required as a matter of law, but he believed that it "added value" to the Authorization for three reasons. First,

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

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

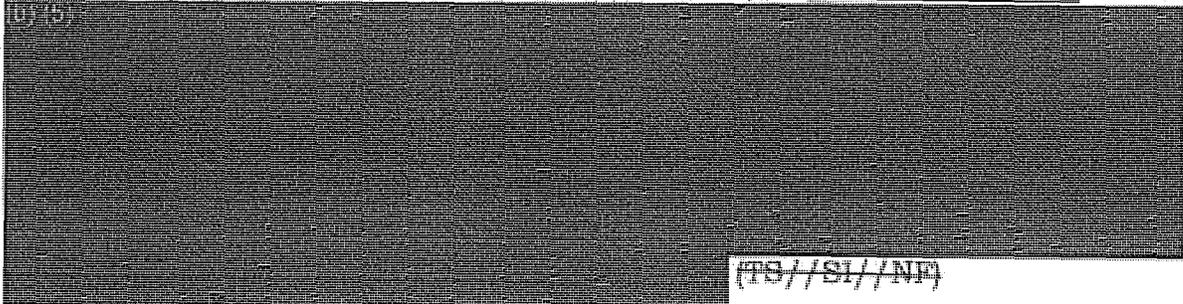
Bybee said that Yoo began working in OLC in July 2001 and that all of the Deputies were in place before Bybee began serving as head of the OLC that November. (U)

Bybee told us he was never read into the Stellar Wind program and could shed no further light on how Yoo came to draft the OLC opinions on the program. However, he said that Yoo had responsibility for supervising the drafting of opinions related to national security issues by the time the attacks of September 11 occurred.³⁰ Bybee described Yoo as “articulate and brilliant,” and also said he had a “golden resume” and was “very well connected” with officials in the White House. He said that from these connections, in addition to Yoo’s scholarship in the area of executive authority during wartime, it was not surprising that Yoo “became the White House’s guy” on national security matters. (U)

b. Yoo’s Legal Analysis of a Warrantless Domestic Electronic Surveillance Program ~~(TS//SI//NF)~~

Before the start of the Stellar Wind program under the October 4, 2001, Presidential Authorization, Yoo drafted a memorandum evaluating the legality of a “hypothetical” electronic surveillance program within the United States to monitor communications of potential terrorists. His memorandum, dated September 17, 2001, was addressed to Timothy Flanigan, Deputy White House Counsel, and was entitled “Constitutional Standards on Random Electronic Surveillance for Counter-Terrorism Purposes.” ~~(TS//STLW//SI//OC/NF)~~

Yoo drafted a more extensive version of this memorandum, dated October 4, 2001, for White House Counsel Gonzales. 



³⁰ As noted above, Yoo, Ashcroft, Card, and Addington declined or did not respond to our request for interviews, and we do not know how Yoo came to deal directly with the White House on legal issues surrounding the Stellar Wind program. In his book “War by Other Means,” Yoo wrote that “[a]s a deputy to the assistant attorney general in charge of the office, I was a Bush Administration appointee who shared its general constitutional philosophy. . . . I had been hired specifically to supervise OLC’s work on [foreign affairs and national security].” John Yoo, *War by Other Means*, (Atlantic Monthly Press, 2006), 19-20. ~~(TS//SI//NF)~~

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

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

Yoo's September 17 and October 4 memoranda were not addressed specifically to the Stellar Wind program, but rather to a "hypothetical" randomized or broadly scoped domestic warrantless surveillance program. As discussed below, the first Office of Legal Counsel opinion explicitly addressing the legality of the Stellar Wind program was not drafted until after the program had been formally authorized by President Bush on October 4, 2001. ~~(TS//SI//OC/NF)~~

Gonzales told the OIG that he did not believe these first two memoranda fully addressed the White House's understanding of the Stellar Wind program. Rather, as described above, these memoranda addressed the legality of a "hypothetical" domestic surveillance program rather than the Stellar Wind program as authorized by the President and carried out by the NSA.³⁵ However, Gonzales also told us that he believed these first two memoranda described as lawful activities that were broader than those carried out under Stellar Wind, and that therefore these opinions "covered" the Stellar Wind program. ~~(TS//SI//NF)~~

2. Presidential Authorization of October 4, 2001

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

On October 4, 2001, President Bush issued the first of 43 Presidential Authorizations for the Stellar Wind program. The October 4 Authorization directed the Secretary of Defense to "use the capabilities of the Department of Defense, including but not limited to the signals intelligence capabilities of the National Security Agency, to collect foreign intelligence by electronic surveillance," provided the surveillance was intended to:

(a) acquire a communication (including but not limited to a wire communication carried into or out of the United States by cable) for which there is probable cause to believe that [REDACTED]

[REDACTED] (b)(1), (b)(3) [REDACTED] a party to such communication is a group engaged in international terrorism, or activities in preparation therefor, or an agent of such a group; or

(b) acquire, with respect to a communication, header/router/addressing-type information, including telecommunications dialing-type data, but not the contents of the communication, when (i) at least one party to such communication is outside the United States or (ii) no party to such communication is known to be a citizen of the United States. ~~(TS//STLW//SI//OC/NF)~~

³⁵ Gonzales noted that Deputy White House Counsel Timothy Flanigan, the recipient of the first Yoo memorandum, was not read into Stellar Wind. ~~(U//FOUO)~~

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

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

Authorization on the spot. According to Baker, Levin also told Baker that when he learned there was no memorandum from the Office of Legal Counsel concerning the program, Levin told Yoo to draft one.

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

Levin's account to us of the instruction that Yoo draft a memorandum concerning the legality of the program differed slightly from Baker's account. Levin told us that he said to Ashcroft that it "wasn't fair" that Ashcroft was the only Justice official read into the program, and that for Ashcroft's protection Levin advised Ashcroft to have another Department official read into the program for the purpose of providing advice on the legality of the program. Levin said he learned that Ashcroft was able to get permission from the White House to have one other person read into the program to advise Ashcroft, although Levin was not certain how Yoo came to be selected as that person.³⁹ As discussed below, Gonzales told us that it was the President's decision to read John Yoo into the program.

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

C. Presidential Authorization is Revised and the Office of Legal Counsel Issues Legal Memoranda in Support of the Program (November 2001 through January 2002)

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

1. Presidential Authorization of November 2, 2001

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

On November 2, 2001, with the first Presidential Authorization set to expire, President Bush signed a second Presidential Authorization. The second Authorization relied upon the same authorities in support of the President's actions, chiefly the Article II Commander-in-Chief powers and the AUMF. The second Authorization cited the same findings in a threat assessment as to the magnitude of the potential threats and the likelihood of their occurrence in the future. However, the scope of authorized content collection and meta data acquisition was redefined by adding the italicized language below in paragraphs 4(a) and (b):

- (a) acquire a communication (including but not limited to a wire communication carried into or out of the United States by cable) for which, *based on the factual and practical considerations of everyday life there are reasonable grounds* to believe that ~~(S)(1), (S)(3)~~

³⁹ By October 4, 2001, Yoo had already drafted two legal analyses on a hypothetical warrantless surveillance program and therefore already had done some work related to the program prior to October 4 when Ashcroft was read in. ~~(TS//SI//NF)~~

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

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

In addition, former OLC Principal Deputy and Acting Assistant Attorney General Steven Bradbury described this [REDACTED]

(b) (5)

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

2. Yoo Drafts Office of Legal Counsel Memorandum Addressing Legality of Stellar Wind

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

The Stellar Wind program was first authorized by President Bush and certified as to form and legality by Attorney General Ashcroft on October 4, 2001, without the support of any formal legal opinion from the Office of Legal Counsel expressly addressing Stellar Wind. ~~(TS//SI//NF)~~

The first OLC opinion directly supporting the legality of the Stellar Wind program was dated November 2, 2001, and was drafted by Yoo. His opinion also analyzed the legality of the first Presidential Authorization and a draft version of the second Authorization.⁴⁰ ~~(TS//SI//NF)~~

In his November 2 memorandum to Attorney General Ashcroft, Yoo opined that the Stellar Wind program ^{(b) (5)} [REDACTED]

As discussed in Chapter Four of this report, however, perceived deficiencies in Yoo's memorandum later became critical to the Office of Legal Counsel's decision to reassess the Stellar Wind program in 2003. We therefore describe Yoo's legal analysis in his November 2 memorandum. ~~(TS//SI//NF)~~

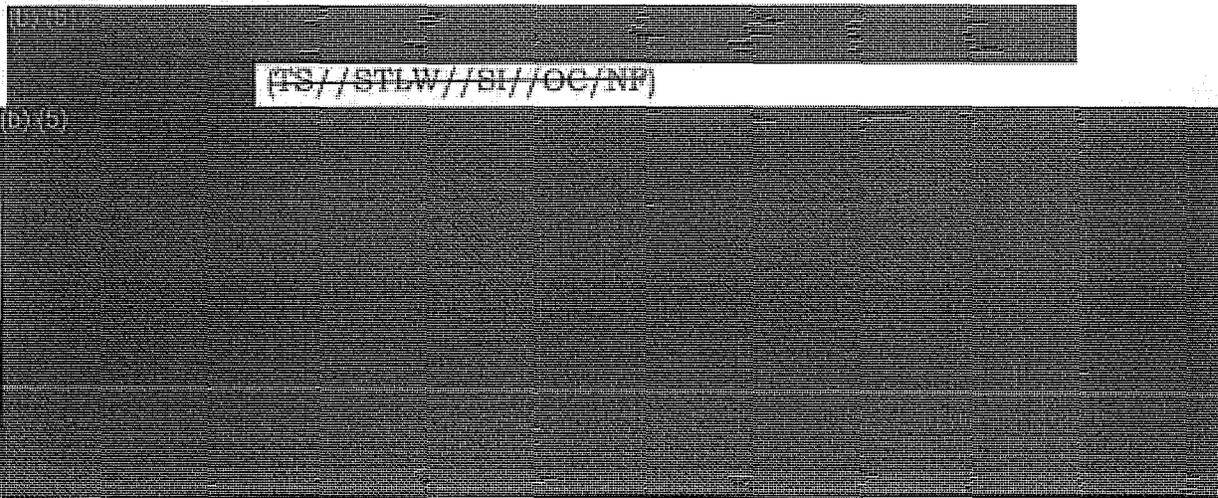
Yoo acknowledged at the outset of his November 2 memorandum that "[b]ecause of the highly sensitive nature of this subject and the time pressures involved, this memorandum has not undergone the usual editing and review process for opinions that issue from our Office [OLC]." The memorandum then reviewed the changes to NSA's collection authority between the first and second Presidential Authorizations. [REDACTED]

(b) (5)

⁴⁰ The second Authorization was issued on November 2, 2001. In developing his legal memorandum, Yoo analyzed a draft of the second Authorization dated October 31, 2001. The OIG was not provided the October 31 draft Presidential Authorization, but based on Yoo's description in his November 2 memorandum, it appears that the draft that Yoo analyzed tracked the language of the final November 2, 2001, Authorization signed by the President. ~~(TS//SI//NF)~~

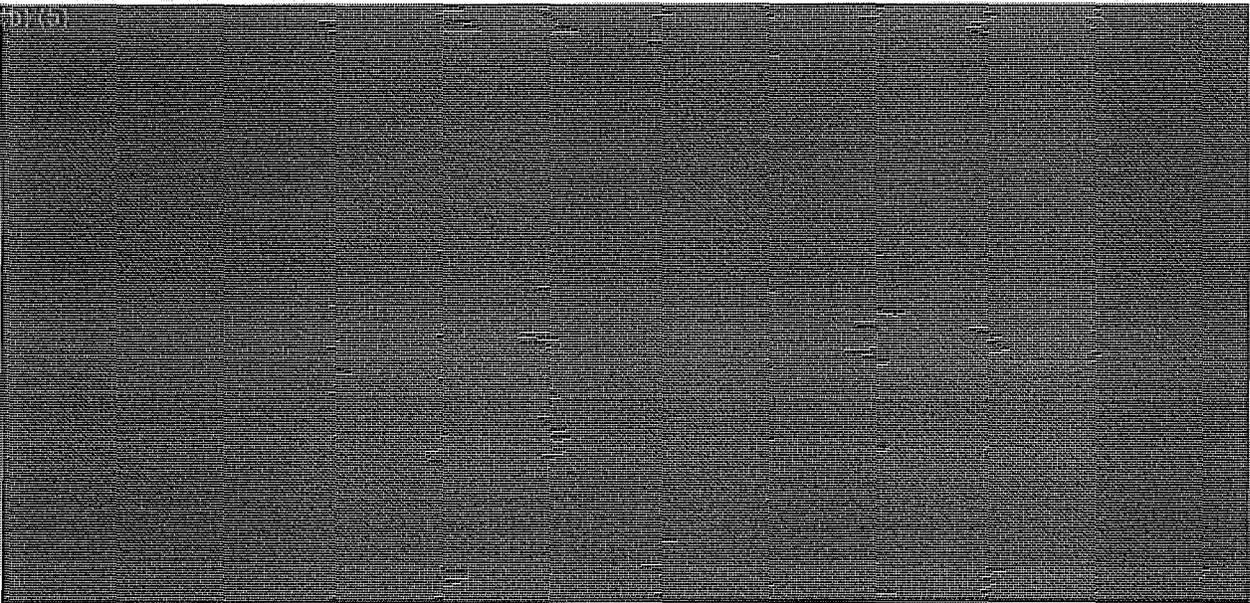
~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

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



Yoo did acknowledge in his memorandum that the first Presidential Authorization was "in tension with FISA." Yoo stated that FISA "purports to be the exclusive statutory means for conducting electronic surveillance for foreign intelligence," but Yoo then opined that "[s]uch a reading of FISA would be an unconstitutional infringement on the President's Article II authorities."⁴¹ Citing advice of the OLC and the position of the Department as presented to Congress during passage of the USA PATRIOT Act several weeks earlier, Yoo characterized FISA as merely providing a "safe harbor for electronic surveillance," adding that it "cannot restrict the President's ability to engage in warrantless searches that protect the national security."

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



⁴¹ As discussed in Chapter Four, Goldsmith criticized this statement as conclusory and unsupported by any separation of powers analysis. (U//~~FOUO~~)

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

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

Regarding whether the activities conducted under the Stellar Wind program could be conducted under FISA, Yoo wrote that it was problematic that FISA required an application to the FISA Court to describe the ~~(b)(1), (b)(3)~~ or "facilities" to be used by the target of the surveillance. Yoo also stated that it was unlikely that a FISA Court would grant a warrant to cover ~~(b)(1), (b)(3)~~ as contemplated in the Presidential Authorization. Noting that the Authorization could be viewed as a violation of FISA's civil and criminal sanctions in 50 U.S.C. §§ 1809-10, Yoo opined that in this regard FISA represented an unconstitutional infringement on the President's Article II powers. According to Yoo, the ultimate test of whether the government may engage in warrantless electronic surveillance activities is whether such conduct is consistent with the Fourth Amendment, not whether it meets the standards of FISA.

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

Citing cases applying the doctrine of constitutional avoidance, Yoo reasoned that reading FISA to restrict the President's inherent authority to conduct foreign intelligence surveillance would raise grave constitutional questions.⁴² Yoo wrote that "unless Congress made a clear statement in FISA that it sought to restrict presidential authority to conduct warrantless searches in the national security area – which it has not – then the statute must be construed to avoid such a reading."⁴³ ~~(TS//STLW//SI//OC/NF)~~

⁴² Yoo's memorandum cited the doctrine of constitutional avoidance, which holds that "where an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress." *Edward J. DeBartolo Corp. v. Florida Gulf Coast Building & Construction Trades Council*, 485 U.S. 568, 575 (1988). Yoo cited cases supporting the application of this doctrine in a manner that preserves the President's "inherent constitutional power, so as to avoid potential constitutional problems." See, e.g., *Public Citizen v. Department of Justice*, 491 U.S. 440, 466 (1989). ~~(TS//STLW//SI//OC/NF)~~

⁴³ On March 2, 2009, the Justice Department released nine opinions written by the OLC from 2001 through 2003 regarding "the allocation of authorities between the President and Congress in matters of war and national security" containing certain propositions that no longer reflect the views of the OLC and "should not be treated as authoritative for any purpose." Steven G. Bradbury, Principal Deputy Assistant Attorney General, Office of Legal Counsel, Department of Justice, Memorandum for the Files, "Re: Status of Certain OLC Opinions Issued in the Aftermath of the Terrorist Attacks of September 11, 2001," January 15, 2009, 1, 11. Among these opinions was a February 2002 classified memorandum written by Yoo which asserted that Congress had not included a clear statement in FISA that it sought to restrict presidential authority to conduct warrantless surveillance activities in the national security area and that the FISA statute therefore does not apply to the president's exercise of his Commander-in-Chief authority. In a January 15, 2009, memorandum (included among those released in March), Bradbury stated that this proposition "is problematic and questionable, given FISA's express references to the President's authority" and is "not supported by convincing reasoning." ~~(TS//STLW//SI//OC/NF)~~

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

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

Yoo's analysis of this point would later raise serious concerns for other officials in the Office of Legal Counsel and the Office of the Deputy Attorney General (ODAG) in late 2003 and early 2004.⁴⁴ Among other concerns, Yoo did not address the 15-day warrant requirement exception in FISA following a congressional declaration of war. See 50 U.S.C. § 1811. Yoo's successors in the Office of Legal Counsel criticized this omission in Yoo's memorandum because they believed that by including this provision in FISA, Congress arguably had demonstrated an intention to "occupy the field" on the matter of electronic surveillance during wartime.⁴⁵

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

Yoo's memorandum next analyzed Fourth Amendment issues raised by the Presidential Authorizations. Yoo dismissed Fourth Amendment concerns regarding the NSA surveillance program to the extent that the Authorizations applied to non-U.S. persons outside the United States. Regarding those aspects of the program that involved interception of the international communications of U.S. persons in the United States, Yoo asserted that Fourth Amendment jurisprudence allowed for searches of persons crossing the border and that interceptions of communications in or out of the United States fell within the "border crossing exception." Yoo further opined that electronic surveillance in "direct support of military operations" did not trigger constitutional rights against illegal searches and seizures, in part because the Fourth Amendment is primarily aimed at curbing law enforcement abuses. ~~(TS//STLW//SI//OC/NF)~~

Finally, Yoo wrote that the electronic surveillance described in the Presidential Authorizations was "reasonable" under the Fourth Amendment and therefore did not require a warrant. In support of this position, Yoo cited Supreme Court opinions upholding warrantless searches in a variety of contexts, such as drug testing of employees and sobriety checkpoints to detect drunk drivers, and in other circumstances "when special needs, beyond the normal need for law enforcement, make the warrant and probable cause requirement impracticable," *Veronia School Dist. 47J v. Acton*, 515 U.S. 464, 652 (1995) (as quoted in November 2, 2001, Memorandum at 20). Yoo wrote that in these situations the government's interest was found to have outweighed the individual's privacy interest, and that in this regard "no governmental interest is more compelling than the security of the Nation." *Haig v. Agee*, 435 U.S. 280, 307 (1981). According

⁴⁴ One of these officials was Patrick Philbin, who following Yoo's departure was "dual-hatted" as both an Associate Deputy Attorney General and a Deputy Assistant Attorney General in the Office of Legal Counsel. (U)

⁴⁵ We discuss the OLC's reassessment and criticism of Yoo's analysis in Chapter Four. (U)

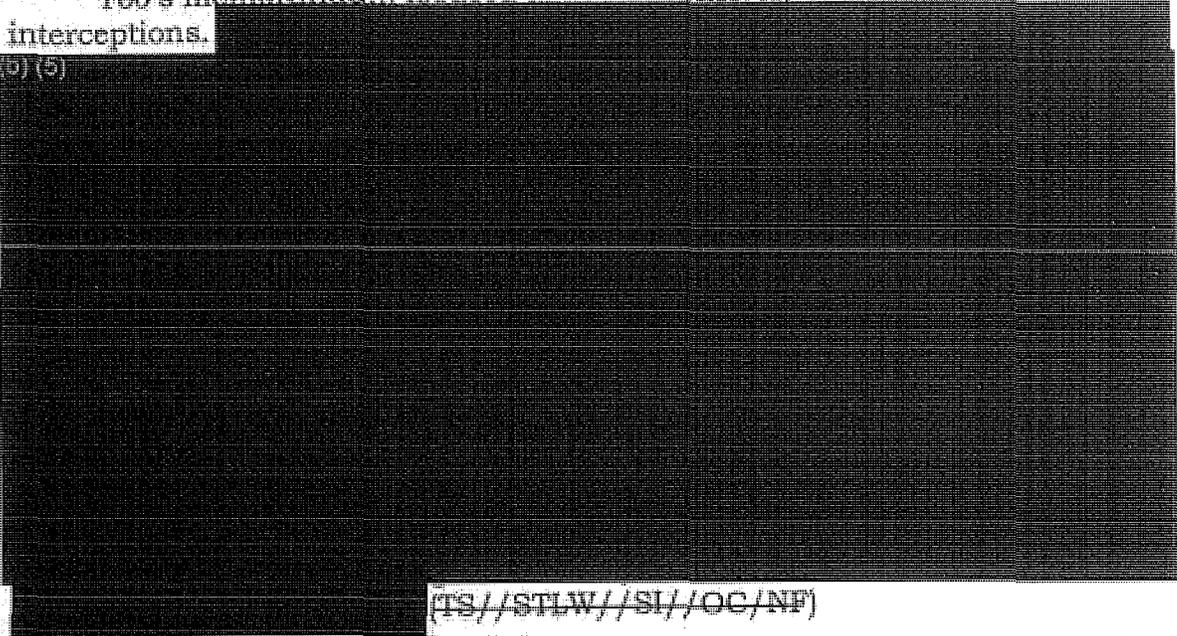
~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

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

to Yoo, the surveillance authorized by the Presidential Authorizations advanced this governmental security interest. ~~(TS//STLW//SI//OC/NF)~~

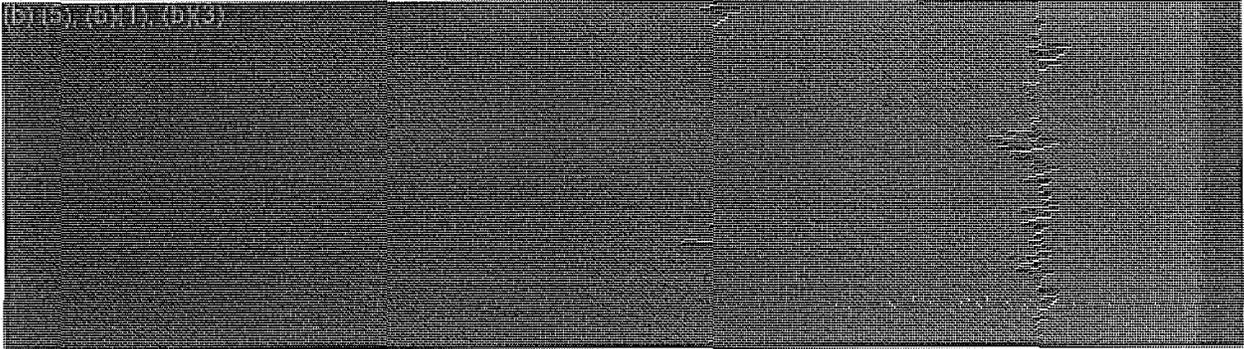
Yoo's memorandum focused almost exclusively on content interceptions.

(b) (5)



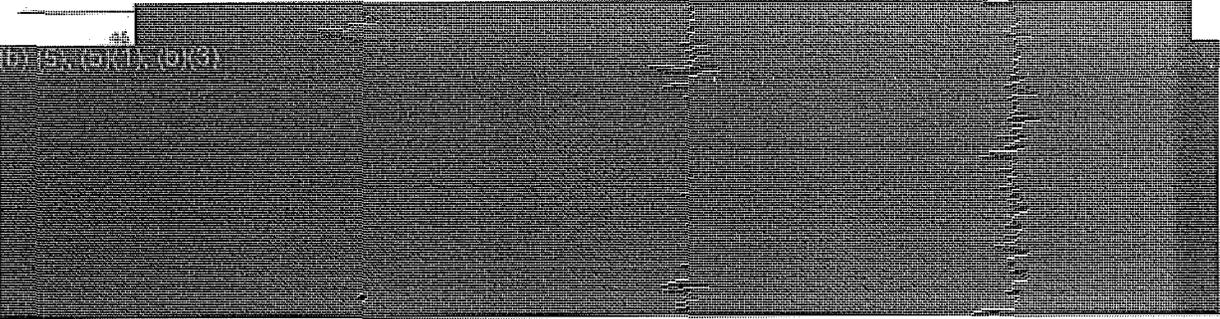
~~(TS//STLW//SI//OC/NF)~~

(b) (5), (b) (1), (b) (3)



Yoo also omitted from his November 2 memorandum – as well as from his earlier September 17 and October 4, 2001, memoranda – any discussion of *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952), a leading case on the distribution of government powers between the Executive and

(b) (5), (b) (1), (b) (3)



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

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

Legislative branches.⁴⁷ As discussed in Chapter Four, Justice Jackson's analysis of President Truman's Article II Commander-in-Chief authority during wartime in the *Youngstown* case was an important factor in the Office of Legal Counsel's reevaluation in 2004 of Yoo's opinion on the legality of the Stellar Wind program. ~~(TS//SI//NF)~~

3. Additional Presidential Authorizations (U)

On November 30, 2001, the President signed a third Authorization authorizing the Stellar Wind program. The third Authorization was virtually identical to the second Authorization of November 2, 2001, in finding that the threat of terrorist attacks in the United States continued to exist, the legal authorities cited for continuing the electronic surveillance, and the scope of collection. ~~(TS//STLW//SI//OC/NF)~~

OLC Principal Deputy and Acting Assistant Attorney General Bradbury told the OIG that

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

Accordingly, the fourth Presidential Authorization, signed on January 9, 2002, modified the scope of collection to provide:

- (a) acquire a communication (including but not limited to a wire communication carried into or out of the United States by cable) for which, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are reasonable grounds to believe such communication originated or terminated outside the United States and a party to such communication is a group

⁴⁷ In *Youngstown*, the Supreme Court held that President Truman's Executive Order directing the Secretary of Commerce to seize and operate steel plants during a labor dispute to produce steel needed for American troops during the Korean War was an unconstitutional exercise of the President's Article II Commander-in-Chief authority. In a concurring opinion, Justice Jackson listed three categories of Presidential actions against which to judge the Presidential powers. First, "[w]hen the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum[.]" Id. at 635. Second, Justice Jackson described a category of concurrent authority between the President and Congress as a "zone of twilight" in which the distribution of power is uncertain and dependant on "the imperatives of events and contemporary imponderables rather than on abstract theories of law." Id. at 637 (footnote omitted). Third, "[w]hen the President takes measures incompatible with the express or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter." Id. Justice Jackson concluded that President Truman's actions fell within this third category, and thus "under circumstances which leave Presidential power most vulnerable to attack and in the least favorable of possible constitutional postures." Id. at 640. (U)

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

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

characterized the collection [REDACTED] and thus their legal advice was based on facts that more closely reflected the actual operation of the program.²²⁵
 (TS//STLW//SI//OC/NF)

In addition, Goldsmith and Philbin discovered that Yoo's assertion that the President had broad authority to conduct electronic surveillance without a warrant pursuant to his Commander-in-Chief powers under Article II of the Constitution, particularly during wartime, never addressed the FISA provision that expressly addressed electronic surveillance following a formal declaration of war. See 50 U.S.C. § 1811. Goldsmith also criticized Yoo's legal memoranda for failing to support Yoo's aggressive Article II Commander-in-Chief theory with a fully developed separation of powers analysis, and instead offering only sweeping conclusions. As an example, Goldsmith cited Yoo's assertion that reading FISA to be the "exclusive statutory means for conducting electronic surveillance for foreign intelligence" amounts to an "unconstitutional infringement on the President's Article II authorities."²²⁶ Moreover, noted Goldsmith, Yoo omitted from his separation-of-powers discussion any analysis of how the Youngstown Steel Seizure Case, a seminal Supreme Court decision on the distribution of governmental powers between the Executive and Legislative Branches during wartime, would affect the legality of the President's actions with respect to Stellar Wind.²²⁷ (TS//STLW//SI//OC/NF)

In reliance on Yoo's advice, the Attorney General certified the program "as to form and legality" some 20 times before Yoo's analysis was determined to be flawed by his successors in OLC and by attorneys in the Office of the Deputy Attorney General. We agree with many of the criticisms offered by Department officials regarding the practice of allowing a single Department attorney to develop the legal justification for the program

[REDACTED]

²²⁵ See Yoo Memorandum, November 2, 2001, at 9. Yoo went on to state that

[REDACTED] Yoo
 concluded that FISA "represents a statutory procedure that creates a safe harbor for surveillance for foreign intelligence purposes." Id. (TS//SI//NF)

²²⁷ The Department's Office of Professional Responsibility (OPR) intends to review whether Yoo's legal analysis concerning the Stellar Wind program violated any standards of professional conduct. OPR has similarly reviewed whether the legal analysis by Yoo and others concerning the detainee interrogation program violated standards of professional conduct. (TS//SI//NF)

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

PREET BHARARA
United States Attorney for the
Southern District of New York
By: DAVID S. JONES
Assistant U.S. Attorney
86 Chambers Street, Third Floor
New York, NY 10007
Tel.: (212) 637-2739
David.Jones6@usdoj.gov

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

.....X
AMERICAN CIVIL LIBERTIES UNION and
THE AMERICAN CIVIL LIBERTIES UNION
FOUNDATION,

Plaintiffs,

v.

13-cv-9198 (AT)

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

.....X

NOTICE OF LODGING OF CLASSIFIED DOCUMENT

Defendants in the above-captioned matter hereby provide notice that, on February 29, 2016, they lodged, for the Court's *in camera, ex parte* review, a classified declaration of David J. Sherman. This document is classified pursuant to Executive Order 13,526, 75 Fed. Reg. 707 (Jan. 5, 2010), and cannot be disclosed without proper authorization. The document was securely transmitted to the Court by Assistant United States Attorney Jean-David Barnea.

Dated: New York, New York
June 8, 2016

Respectfully submitted,

PREET BHARARA
United States Attorney for the
Southern District of New York

By: /s/ David S. Jones
DAVID S. JONES
Assistant United States Attorney
86 Chambers Street, Third Floor
New York, New York 10007
Telephone: (212) 637-2739
Facsimile: (212) 637-2730
David.Jones6@usdoj.gov

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

AMERICAN CIVIL LIBERTIES UNION, and)
AMERICAN CIVIL LIBERTIES UNION)
FOUNDATION,)
) Case No. 13-cv-9198 (AT)
Plaintiffs,)
)
v.)
)
NATIONAL SECURITY AGENCY,)
CENTRAL INTELLIGENCE AGENCY,)
DEPARTMENT OF DEFENSE,)
DEPARTMENT OF JUSTICE, and)
DEPARTMENT OF STATE,)
)
Defendants.)
_____)

SUPPLEMENTAL DECLARATION OF DAVID J. SHERMAN

I, DAVID J. SHERMAN, hereby declare and state:

1. Please refer to the UNCLASSIFIED Declaration of David J. Sherman, dated 26 February 2016, for a summary of my background, my role as a TOP SECRET original classification authority (“OCA”), the National Security Agency’s (“NSA” or “Agency”) origin and mission, and the importance of SIGINT to the national security.

2. The declaration supplements my CLASSIFIED and UNCLASSIFIED declarations of 26 February 2016. The purpose of this declaration is to provide additional information regarding certain withholdings taken by the NSA that have been challenged by Plaintiffs, the American Civil Liberties Union and the American Civil Liberties Union Foundation (collectively, “Plaintiffs” or “ACLU”).

Legal Memoranda Withheld in Full Under Exemptions 1 and 3

3. ACLU has challenged NSA’s withholding in full of certain legal memoranda, arguing that it appears that the Agency claimed Exemptions 1 and 3 over only portions of the memoranda while improperly claiming Exemption 5 over the entirety of the memoranda. The

NSA documents falling within this category include NSA Documents 7, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21.

4. As previously explained in my 26 February 2016 UNCLASSIFIED declaration at paragraphs 38-52 and 54 and my CLASSIFIED declaration at paragraphs 7-11, the legal analyses in all of the memoranda and opinions that Plaintiffs are challenging in this category are inextricably intertwined with factual descriptions of NSA functions and activities that are both classified and protected from public disclosure by statute. The mere subject matter of these memoranda and opinions pertains to classified NSA operations and activities that have not been publicly acknowledged. The release of even the basic factual or legal background in these memoranda could reasonably be expected to cause harm to the national security or an interest protected by statute, as the formulation of the legal analysis itself could enable Plaintiffs and the public to discern classified or protected facts about the program or activity being discussed. Indeed, even the title and subject matter of these documents would tend to reveal classified and protected information about NSA functions and activities. As a result, I have determined that no portion of these documents could reasonably be segregated and released. Further, even if the working law doctrine were applicable here, which is not the case, the fact that the challenged redactions are currently and properly classified matters in accordance with E.O. 13526 and protected from release by statute means that the information continues to be properly withheld. *See N.Y. Times Co. v. U.S. Dep't of Justice*, 806 F.3d 682, 687 (2d Cir. 2015).

5. By contrast, NSA assessed and determined that certain of the factual discussion in the memorandum identified as NSA 28 is UNCLASSIFIED and not inextricably intertwined with the legal analyses contained therein. Moreover, the subject matter of NSA 28 – the sharing of raw signals intelligence through database access with personnel from other U.S. government agencies – has been publicly acknowledged by NSA and is considered to be UNCLASSIFIED. Consequently, unlike NSA documents 7, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, and 21, NSA

determined that portions of NSA 28 were reasonably segregable and releasable in part. In a similar vein, OLC 3, 4, 6, 8, and NSD 36 also relate to subjects that have been publicly acknowledged by NSA. The Department of Justice's Office of Legal Counsel has explained its justification for withholding these documents in their entirety based on FOIA Exemption 5. In addition to OLC's withholdings, I have also determined that certain information in these documents may be independently withheld pursuant to FOIA Exemptions 1 and 3 because the information is currently and properly classified in accordance with E.O. 13526 and protected from release by statute. It is my assessment, however, that these documents also contain some reasonably segregable UNCLASSIFIED information that could not be withheld based on Exemptions 1 and 3.¹

6. As discussed in paragraphs 40, 46, and 47 of my 26 February 2016 UNCLASSIFIED declaration, the information contained in the challenged documents is currently and properly classified at levels ranging from SECRET to TOP SECRET because the release of this information could reasonably be expected to cause serious to exceptionally grave damage to the national security. The NSA withholdings in the documents challenged in this category describe both classified and protected information regarding NSA information assurance and network defense activities, SIGINT collection activities and access points, uses of particular SIGINT collection, and NSA's relationships with partners and providers. The damage to national security that reasonably could result from disclosure of this information is described in detail in paragraphs 39 and 48 of my 26 February 2016 UNCLASSIFIED declaration and paragraph 9 of my CLASSIFIED declaration. Therefore, this information meets the criteria for classification set forth in Sections 1.4(c), 1.4(d), and 1.4(g) of Executive Order 13526.

¹ As I stated in my prior UNCLASSIFIED declaration to this Court, should the Court determine that the information in these documents was not properly withheld in full under Exemption 5, NSA will segregate and release all non-exempt information in these documents.

7. Additionally, this same information is protected from released under FOIA Exemption 3, as described in paragraphs 41-44 and 49-52 of my 26 February 2016 UNCLASSIFIED declaration. This information is protected from release by Section 6 of the National Security Agency Act of 1959 (50 U.S.C. § 3605) because it involves a “function of the [NSA], or...information with respect to the activities thereof.” The information is further protected based on Section 102A(i)(1) of the National Security Act of 1947, as amended, which states that the Director of National Intelligence “shall protect intelligence sources and methods from unauthorized disclosure.” 50 U.S.C. § 2034(i)(1). Finally, this information is protected from release under 18 U.S.C. § 798, which protects from disclosure information concerning the communications intelligence activities of the United States, or information obtained by communications intelligence processes. As discussed in detail above in paragraph 4, the release of any portion of these memoranda and opinions would enable Plaintiffs and the public to discern information about NSA programs, operations, and activities that is both classified and protected from disclosure by these three statutes. As a result, no portion of the documents in this category can be segregated and released without disclosing protected information.

Inspector General and Compliance Reports

8. ACLU has also challenged NSA’s withholding of certain numbers (to include the numbers of compliance incidents) from an NSA intelligence oversight board report (NSA 79). As previously explained in my declaration dated 26 February 2016, and as explained in greater detail below, the disclosure of such information would reveal the overall scope of NSA’s foreign intelligence collection efforts, to include NSA’s ability to collect specific foreign intelligence information. The disclosure of this information would also reveal gaps in NSA’s collection capabilities. Such information concerns core NSA functions and activities – the collection, analysis, and dissemination of foreign intelligence information derived from signals intelligence obtained pursuant to E.O. 12333 and, by law, is exempt from disclosure. Further, a subset of the

withheld information is classified as its public disclosure would be reasonably likely to damage national security.

9. Specifically, this information is protected from release under FOIA Exemption 3, as described in paragraph 68 of my 26 February 2016 UNCLASSIFIED declaration. This information is exempt from release under Section 6 of the National Security Agency Act of 1959 (50 U.S.C. § 3605), which protects from disclosure “the organization or any function of the National Security Agency, [or] of any information with respect to the activities thereof” Although in this case, the disclosure of the withheld information reasonably could be expected to cause damage or serious damage to the national security, to invoke Section 6, NSA must demonstrate only that the information it seeks to protect falls within the scope of the statute, and is not required to demonstrate a specific harm to national security.

10. In this case, the withheld numbers all relate to NSA’s collection, analysis, and dissemination of signals intelligence for foreign intelligence purposes and the manner in which NSA conducts compliance and oversight over that SIGINT mission. As such, the withheld information falls squarely within the scope of Section 6 as it relates to both a core Agency function, its SIGINT mission, and the compliance and oversight activities conducted in support thereof.

11. In addition to being exempt from disclosure by statute, much of the withheld information that falls into this category is also protected as classified pursuant to FOIA Exemption 1. For example, NSA withheld each number that would reveal the number of times that a particular compliance incident was documented during the timeframe of the intelligence oversight board report. It did so because the disclosure of such numbers, in compilation with information that has been previously released, would tend to disclose the overall scope of NSA’s foreign intelligence collection efforts. This information, if released, could be pieced together to reveal highly sensitive information to our adversaries. For example, the number of compliance incidents could permit our adversaries to determine the scope of NSA’s collection activities under particular programs

and/or NSA's ability and accuracy in determining the "foreignness" of the selectors targeted for acquisition. Other withheld numbers would allow an adversary to assess which NSA capabilities the Agency uses most frequently, and in turn to assess which of their communications may or may not be secure. Adversaries could then take countermeasures to prevent the NSA from collecting their communications, such as changing methods of communication to one more difficult for NSA to intercept or engaging in tradecraft to avoid NSA collection. As a result, NSA could potentially lose valuable sources of intelligence unless and until the Agency is able to identify a replacement source. In compilation, the numbers that were withheld for classification purposes would disclose the overall scope of NSA's E.O. 12333 collection capabilities.

12. Accordingly, I have determined that the specific numbers that NSA withheld pursuant to FOIA Exemption 1 pertain to intelligence activities, intelligence sources or methods, or cryptology, or the vulnerabilities or capabilities of systems or projects relating to the national security and therefore meet the criteria for classification set forth in sections 1.4(c) and 1.4(g) of E.O. 13526. This information is currently and properly classified at levels ranging from CONFIDENTIAL to SECRET because the release of this information could reasonably be expected to cause damage or serious damage to the national security. Finally, in accordance with Section 1.7 of E.O. 13526, no information was classified and withheld in order to conceal violations of law or to prevent embarrassment to the Agency.

13. ACLU is also challenging the withholding in full of NSD documents 7, 37, 42, 44, and 47. As discussed in detail in my classified declaration, these documents concern in their entirety specific classified operations or activities of the Agency that have not been publicly acknowledged and do not contain any segregable information. The compliance matters discussed therein are inextricably intertwined with factual descriptions of NSA functions and activities that are both classified and protected from public disclosure by statute. As a result, I have determined that no portion of these documents could reasonably be segregated and released. NSA 79, in

contrast, generally describes a number of different compliance-related matters reported to NSA's overseers pursuant to E.O. 12333. During its review, NSA determined that it could segregate and release UNCLASSIFIED materials from NSA 79 (to include publicly acknowledged NSA functions and activities) while protecting the material that remains classified and/or protected from disclosure by law, to include factual descriptions of specific NSA operations or activities that have not been publicly acknowledged.

Documents Characterized by Plaintiffs as Containing "Working Law"

14. NSA 28 is a legal opinion drafted by the NSA OGC at the request of its client, the NSA's Signals Intelligence Directorate ("SID"). My purpose herein is to provide the court with a more fulsome factual description of NSA 28. Portions of NSA 28 were properly redacted as attorney-client privileged information and should not be considered "working law" of the NSA. NSA 28 sets out legal advice concerning the legal limits to access by non-NSA personnel of NSA signals intelligence databases. The document further provides legal advice regarding the constitutional and statutory privacy protections that constrain access to such databases depending on whether the databases contain content or metadata. Finally, the document describes potential changes to existing NSA dissemination procedures that OGC anticipated might be proposed and provides OGC views and recommendations regarding such potential changes.²

15. NSA 28 is, at its core, legal advice offered by the NSA OGC to its client, NSA's SID, at the client's request. It is a legal memorandum that describes the legal advisability or permissibility of possible policies, but does not authoritatively state or determine NSA's policy. The document sets forth an NSA attorney's analysis of the legal boundaries for a particular NSA

² A similar rationale also applies to NSA Documents 11, 12, and 16. As described above, however, the very subject matter of NSA 11, 12, and 16 is classified and properly protected by law from public disclosure. Accordingly, nothing more can be said of these documents on the public record.

activity, but does not constitute a final Agency decision nor should it be considered binding NSA policy. As a matter of policy, SID could implement the sharing of raw SIGINT database access to non-NSA personnel in any number of possible ways, to include deciding to not implement any such access. The NSA OGC's advice was not binding upon SID, and that component was free to decline to adopt any of the dissemination practices discussed in the memorandum.

16. Moreover, the NSA OGC is not authorized to make decisions about SID policy nor can the OGC legal opinion be considered an authoritative statement of SID policy. The NSA OGC is the exclusive NSA component for providing legal services to all NSA elements and is led by the General Counsel, who is the NSA's chief legal officer. The office provides legal advice on a number of different legal matters, but the office has no authority to issue final decisions or authoritative statements on NSA policy, to include NSA's implementation of raw SIGINT database access by non-NSA personnel. The NSA OGC opinion merely amounts to advice offered by that office for consideration by personnel within the NSA SID. In short, the memorandum addresses the legal advisability and/or permissibility of anticipated policy changes but is neither authoritative nor determinative of NSA's policy in this regard. Consequently, NSA 28 should not be considered the "working law" of NSA.³

³ ACLU's opposition also called to NSA's attention that there may be inconsistencies to information redacted from a 1988 version of the Classified Annex to DoD Procedures Under E.O. 12333, ACLU Memorandum of Law at 42 (citing Exs. L and M. to Manes Decl.) (NSD 94-125), with a document issued subsequent to the Classified Annex. NSA is reviewing ACLU's assertions and hopes to complete its assessment within 30 days.

CONCLUSION

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed this 7th day of June, 2016, pursuant to 28 U.S.C. § 1746.



Dr. David J. Sherman
Associate Director for Policy and Records,
National Security Agency

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

AMERICAN CIVIL LIBERTIES UNION
and AMERICAN CIVIL LIBERTIES
UNION FOUNDATION,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY,
CENTRAL INTELLIGENCE AGENCY,
DEPARTMENT OF DEFENSE,
DEPARTMENT OF JUSTICE, and
DEPARTMENT OF STATE,

Defendants.

Civil Action No. 13-CV-9198 (AT)

DECLARATION OF JOHN BRADFORD WIEGMANN

I, John Bradford Wiegmann, declare as follows:

1. I am a Deputy Assistant Attorney General in the National Security Division (“NSD”) of the United States Department of Justice (“DOJ” or “Department”). NSD is a component of the Department which formally began operations on October 2, 2006, by consolidating the resources of the Office of Intelligence Policy and Review (“OIPR”) and the Criminal Division’s Counterterrorism Section (“CTS”) and Counterespionage Section (“CES”).

2. In my capacity as Deputy Assistant Attorney General, I supervised the Freedom of Information (“FOIA”) and Declassification Unit, which is responsible for responding to requests for access to NSD records and information pursuant to the FOIA, 5 U.S.C. § 552 and the Privacy Act of 1974.¹ The FOIA and Declassification Unit also processes the NSD records

¹ The FOIA and Declassification Unit is now supervised by the Director of Risk Management and Development.

which are responsive to FOIA requests received by other Executive Branch agencies. In addition, I am responsible for overseeing NSD's Law and Policy Office, which implements Department of Justice policies with regard to intelligence, counterterrorism, and other national security matters and provides legal assistance and advice on matters of national security law. The statements contained in this declaration are based upon my personal knowledge, information provided to me in the course of my official duties, and determinations I have made following a review of NSD's potentially responsive documents.

3. In a letter dated, May 13, 2013, plaintiff, the American Civil Liberties Union ("ACLU") requested the following:

- (1) Any records construing or interpreting the authority of the National Security Division ("NSD") under Executive Order 12,333 or any regulations issued thereunder;
- (2) Any records describing the minimization procedures used by the NSD with regard to both intelligence collection and intelligence interception conducted pursuant to the NSD's authority under EO 12,333 or any regulations issued thereunder; and
- (3) Any records describing the standards that must be satisfied for the "collection," "acquisition," or "interception" of communications, as the NSD defines these terms, pursuant to the NSD's authority under EO 12,333 or any regulations issued thereunder.

This request was assigned NSD FOI/PA #13-175.

4. ACLU served its complaint in this lawsuit on the United States Attorney for the Southern District of New York on December 30, 2013.

5. In a letter dated, May 14, 2014, NSD informed plaintiff that Executive Order 12333 governs intelligence collection by intelligence agencies, and that because NSD is not an intelligence agency, it does not collect intelligence. In addition, NSD stated that it has no authority under Executive Order 12333, and, as a result, NSD possessed no responsive records.

6. In a letter dated July 29, 2014, ACLU submitted a new request for the following information:

- (1) Formal regulations or policies relating to any agency's authority under EO 12,333 to undertake "Electronic Surveillance" (as that term is defined in EO 12,333) that implicates "United States Persons" (as that term is defined in EO 12,333), including regulations or policies relating to the acquisition, retention, dissemination, or use of information or communications to, from, or about United States Persons under such authority.
- (2) Records that officially authorize or modify under EO 12,333 any agency's use of specific programs, techniques, or types of Electronic Surveillance that implicate United States Persons, including official rules or procedures for the acquisition, retention, dissemination, or use of information or communications to, from, or about United States persons under such authority generally or in the context of particular programs, techniques, or types of Electronic Surveillance.
- (3) Formal legal opinions addressing any agency's authority under EO 12,333 to undertake specific programs, techniques, or types of Electronic Surveillance that implicate United States Persons, including formal legal opinions relating to the acquisition, retention, dissemination, or use of information or communications to, from, or about United States Persons under such authority generally or in the context of particular programs, techniques, or types of Electronic Surveillance.
- (4) Formal training materials or reference materials (such as handbooks, presentations, or manuals) that expound on or explain how any agency implements its authority under EO 12,333 to undertake Electronic Surveillance that implicates United States Persons, including the acquisition, retention, dissemination, or use of information or communications to, from, or about United States Persons under such authority.
- (5) Formal reports relating to Electronic Surveillance under EO 12,333 implicating United States Persons that contain any meaningful discussion of (1) any agency's compliance, in undertaking such surveillance, with EO 12,333, its implementing regulations, the Foreign Intelligence Surveillance Act, or the Fourth Amendment; or (2) any agency's interception, acquisition, scanning, or collection of the communications of United States Persons, whether "incidental" or otherwise, in undertaking such surveillance; and that are or were:

- (a) Authored by an inspector general or the functional equivalent thereof;
- (b) Submitted to Congress, the Office of the Director of National Intelligence, the Attorney General, or the Deputy Attorney General;
- or
- (c) Maintained by the office of the Assistant Attorney General for National Security.

This request was assigned NSD FOI/PA #14-177.

7. On October 31, 2014, ACLU filed an amended complaint, which made the July 29, 2014 request a part of the December 30, 2013 lawsuit.

8. As discussed in my February 26, 2016 declaration, NSD located 68 responsive records; eight of those records were released in full to plaintiffs, nine were released in part, and the remaining 51 were withheld in full. Plaintiffs indicated that they wished to challenge only some of the documents withheld in full: NSD Document Numbers 2, 4, 7, 9, 12, 13, 14, 17, 18, 23, 30, 31, 33, 36, 37, 42, 44, 47, and 48. Plaintiffs also challenged the partial withholding of the documents Bates numbered NSD 94-125 and NSD 202-207. These documents were described in an index attached to that declaration.

9. I have reviewed and am familiar with all of the documents discussed above, including NSD Document 4. NSD Document 4 was withheld in full pursuant to FOIA Exemptions 1 and 3 and Exemption 5 under the deliberative process privilege and the attorney client privilege. My February 26, 2016 declaration and the Vaughn index attached to it describe the privileged nature of NSD Document 4.

10. NSD Document 4 is an NSD legal memorandum regarding amending Department of Defense (“DOD”) procedures, along with accompanying documentation. The memorandum recommends that the Attorney General approve the amendment to the DOD procedures. NSD

Document 4 is a recommendation memo; it does not have the force and effect of law within the Department, and it has not been adopted by the Department as a governing policy. Therefore, NSD Document 4 is not “working law.” Further, I am unaware of any official acknowledgment or release of NSD Document 4.

11. In addition, as described in my February 26, 2016 declaration, NSD conducted a search for responsive documents after identifying and then directing six attorneys in NSD’s Office of Intelligence² and one attorney in the NSD’s Office of Law and Policy³ who have worked on issues concerning electronic surveillance under Executive Order 12333 described in the request to conduct searches for responsive documents. Due to the nature of their duties, no other NSD personnel were likely to have responsive records that at least one of these seven attorneys did not also have. The six attorneys within NSD’s Office of Intelligence consisted of some of the most senior and knowledgeable attorneys within that office, each having extensive institutional knowledge and supervisory responsibilities. These attorneys were (1) a Counsel to the Assistant Attorney General, (2) the Section Chief of Operations, (3) the Section Chief of Oversight, (4) a Deputy Section Chief of Operations, (5) a second Deputy Section Chief of Operations, and (6) a Unit Chief of Operations. These six attorneys oversaw all of the work OI did on matters pertaining to Executive Order 12333, and any additional records possibly located in the files of another OI employee would likely have been duplicated in the files of at least one of these six attorneys. In addition, NSD searched the records of the Special Counsel within the Office of Law and Policy. Prior to working in the Office of Law and Policy, the Special Counsel

² NSD’s Office of Intelligence ensures that the Intelligence Community agencies have the legal authorities necessary to conduct intelligence operations, particularly operations involving the Foreign Intelligence Surveillance Act (FISA); that the office exercises meaningful oversight over various national security activities of Intelligence Community agencies; and that it can play an effective role in FISA-related litigation.

³ NSD’s Law and Policy Office develops and implements Department of Justice policies with regard to intelligence, counterterrorism, and other national security matters and provides legal assistance and advice on matters of national security law.

worked as a Deputy Counsel in OIPR⁴, and he is among the most knowledgeable attorneys in the Office of Law and Policy on surveillance matters. Because of this, he continues to work on and advise others working on critical surveillance related matters as a Special Counsel in the Office of Law and Policy. In addition, the Special Counsel works more on 12333 related matters than anyone else in the Office of Law and Policy. As a result, it is unlikely that any additional significant records would be located in the files of another employee within the Office of Law and Policy. Further, NSD FOIA staff also conducted a historical search of OIPR's policy files for any potentially responsive records generated before the formation of the National Security Division. These searches captured all the systems and types of files that were likely to contain responsive records possessed by each attorney, and NSD FOIA is unaware of other locations or personnel that would be likely to yield additional responsive information.

12. Further, because NSD Documents 12, 13, 14, 23, and 33 and NSA Documents 11 and 12 are classified, this declaration cannot provide additional information further justifying why the memoranda contained within are protected by the attorney-client privilege. But I reaffirm the explanation in paragraph 15 of my February 26, 2016 declaration that the memoranda within all of these documents are properly protected by the attorney-client privilege. I respectfully refer this Court to my February 26, 2016 declaration and to the Classified Declaration of David J. Sherman for additional information.

13. Additionally, attached to this declaration is a true and correct copy of NSD's May 1, 2015 transmittal letter to plaintiffs which discusses withholdings under multiple FOIA exemptions, including FOIA Exemption (b)(6).

⁴ OIPR was the predecessor organization of NSD's Office of Intelligence.

CONCLUSION

I certify, pursuant to 28 U.S.C. § 1746, under penalty of perjury that the foregoing is true and correct.

Executed this 8th day of June 2016, Washington, DC


JOHN BRADFORD WIEGMANN

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

AMERICAN CIVIL LIBERTIES UNION, and)
AMERICAN CIVIL LIBERTIES UNION)
FOUNDATION,)

Plaintiffs,)

v.)

NATIONAL SECURITY AGENCY,)
CENTRAL INTELLIGENCE AGENCY,)
DEPARTMENT OF DEFENSE,)
DEPARTMENT OF JUSTICE, and)
DEPARTMENT OF STATE,)

Defendants.)

Case No. 13-cv-9198 (KMW)(JF)

SUPPLEMENTAL DECLARATION OF DAVID J. SHERMAN

I, DAVID J. SHERMAN, hereby declare and state:

1. Please refer to my UNCLASSIFIED Declaration in this case (Dkt. No. 64), dated 26 February 2016, for a summary of my background, my role as a TOP SECRET original classification authority (“OCA”), the National Security Agency’s (“NSA” or “Agency”) origin and mission, and the importance of SIGINT to the national security.

2. This declaration¹ supplements my CLASSIFIED and UNCLASSIFIED¹ declarations of 26 February 2016, as well as my UNCLASSIFIED Supplemental Declaration of 7 June 2016 (Dkt. No. 79). The purpose of this declaration is to provide additional information regarding certain withholdings taken by the NSA that have been challenged by Plaintiffs, the American Civil Liberties Union and the American Civil Liberties Union Foundation (collectively,

¹ Referenced in Dkt. No. 74, Notice of Filing of Classified Document.

“Plaintiffs” or “ACLU”), in response to the Court’s Memorandum Opinion and Order of 27 March 2017.

Legal Memoranda Withheld Pursuant to Exemption 5

3. NSA withheld in full NSA Documents 7, 11, 12, and 14-21 and withheld in part NSA Document 28 pursuant to Exemption 5 of the FOIA.² NSA also withheld NSA Documents 7, 11, 12, and 14-21 in full pursuant to Exemptions 1 and 3 of the FOIA.³ ACLU challenged these withholdings. The Court denied Defendants’ motion for summary judgment concerning these materials and invited Defendants to supplement their submissions with regard to these documents concerning Exemption 5 applicability. The Court, however, upheld NSA’s withholdings of those documents withheld in full pursuant to Exemptions 1 and 3 (Mem. at 36); accordingly, this submission addresses only Exemption 5 in the context of these specified legal memoranda.

4. With respect to NSA Documents 11 and 12, the Court noted that given the description of the materials contained therein, “[w]ithout more, Defendants cannot satisfy their burden that Exemption 5 applies to these two documents” (*Id.* at 29). As in Defendants’ prior submissions, it is my understanding that NSD will continue to justify the applicability of the Attorney-Client and Deliberative Process Privileges under FOIA Exemption 5 to NSA Documents 11 and 12, providing such information in a supplemental declaration separate and apart from the instant submission. (*See, e.g.*, NSA Decl., Dkt. No. 64, ¶ 25).⁴

² Capitalized terms and abbreviations not defined herein were defined in my previous declarations.

³ As noted in my prior UNCLASSIFIED declaration, with respect to the redacted information in NSA Document 28, “[a]ll information withheld pursuant to Exemption 5 is independently exempt from public release based on Exemptions 1 and/or 3 of the FOIA.” (NSA Decl., Dkt. No. 64, ¶ 55; *see also id.* n.7).

⁴ Defendants also asserted the Presidential Communications Privilege under FOIA Exemption 5 with respect to portions of NSA Document 12, which was upheld by the Court. (Mem. at 30).

5. NSA also asserted Attorney-Client Privilege regarding NSA Documents 7, 14, 15, 16, 17, 18, 19, 20, 21, and 28. With respect to these materials, in NSA's initial submission, I explained that these documents "have not since been used to publically justify NSA actions or expressly adopted as Agency policy." (NSA Decl., Dkt. No. 64, ¶ 53). While the Court was "satisfied that these documents are protected by attorney-client privilege," it nevertheless denied Defendants' motion for summary judgment on Exemption 5, as it could not "determine whether these documents contain working law or have not been adopted." (Mem. at 30). In particular, the Court held that NSA stated the rule concerning working law "too narrowly," by not acknowledging the possibility of informal, non-public adoption. (*Id.*). As a matter of further clarification, the materials constituting NSA Documents 7, 14-21, and 28, described in detail *infra*, reflect legal advice that constitutes one consideration, of many, for decisionmakers; these memoranda do not reflect the Agency's final decision to engage in a particular course of action or to adopt a particular policy, either formally or informally. At bottom, as these memoranda have "no operative effect," they need not be disclosed "even where the agency action agrees with the conclusion of the report or recommendation." (*Id.* at 20 (citing *Brennan Ctr. for Justice v. U.S. Dep't of Justice*, 697 F.3d 184, 196 (2d Cir. 2012) (citations and quotations omitted))). None of these memoranda, which are patently advisory in nature, reflect binding statements of NSA's legal position, definitive statements of NSA policy, or final determinations with any operative effect. I will address each memorandum briefly in turn, so as to provide the court with a more complete description of the material and facilitate any further analysis of Exemption 5.

6. NSA Document 7 is a legal memorandum to a Deputy General Counsel of NSA written by a senior NSA intelligence law attorney concerning a classified NSA SIGINT activity. The memorandum was provided to this Deputy General Counsel in order to provide updated

information concerning past legal advice regarding the parameters of certain classified SIGINT activity.

7. NSA Document 14 is a legal memorandum written by a senior NSA intelligence law attorney for NSA's former Signals Intelligence Directorate (SID)⁵ concerning classified SIGINT activities and reflects legal advice concerning a range of options to be considered by decisionmakers.

8. NSA Document 15 is a legal memorandum written by a senior NSA intelligence law attorney for the Director of SID concerning classified NSA activities and is informational in nature. It does not reflect a decision to engage in a particular course of action, but rather, constitutes recommendations from the attorney to the SID.

9. NSA Document 16 is a legal memorandum written by a senior NSA intelligence law attorney providing legal advice to the SID concerning classified activities undertaken pursuant to EO 12333 and reflects non-binding, attorney guidance.

10. NSA Document 17 is a legal memorandum written by a senior NSA intelligence law attorney for the Director of SID concerning audits of SIGINT activities undertaken pursuant to EO 12333. The memorandum constitutes recommendations and analysis provided by the senior attorney in response to a request for legal advice.

11. NSA Document 18 is a legal memorandum written by a senior NSA intelligence law attorney for NSA senior leadership concerning the protection of US Person information under EO 12333 and related regulations. The memorandum presents multiple points of consideration for leadership in its analysis, and reflects the attorney's legal interpretation of various aspects of the questions presented.

⁵ In August 2016, NSA reorganized. Functions of the SID, to include the SIGINT activities in NSA 14, now reside with NSA's Operations Directorate.

12. NSA Document 19 is a legal memorandum written by a senior NSA intelligence law attorney for the SID concerning the protection of US Person information during classified SIGINT activities undertaken pursuant to EO 12333. The memorandum contains legal conclusions concerning these issues and reflects recommendations to decisionmakers.

13. NSA Document 20 is a legal memorandum written by a senior NSA intelligence law attorney for the SID concerning querying data collected pursuant to EO 12333. This memorandum is informational in nature and reflects legal advice concerning certain queries of this data. The memorandum contains recommendations for consideration concerning such queries.

14. NSA Document 21 is a legal memorandum written by a senior NSA intelligence law attorney for the SID concerning NSA's authority to conduct certain classified SIGINT activities. The memorandum reflects legal interpretations of the regulatory environment and provides clarifications regarding NSA authority, and also presents recommendations for future.

15. With respect to NSA Document 28, I discussed this document in detail in my Supplemental Declaration of 7 June 2016, noting that NSA 28 is a "legal opinion drafted by the NSA OGC at the request of its client," the SID. (NSA Supp. Decl., Dkt. No. 79, ¶¶ 14-16). In particular, I explained that the redacted attorney-client privileged information should not be considered "working law" of the NSA, as the memorandum instead "sets out legal advice concerning the legal limits to access by non-NSA personnel of NSA signals intelligence databases," as well as advice concerning privacy protections and "potential changes to existing NSA dissemination procedures." (*Id.* ¶ 14). As this document was never binding upon SID, which "was free to decline to adopt any of the dissemination practices discussed in the memorandum" (*id.* ¶ 15), it too reflects considerations for decisionmakers rather than itself constituting a binding policy determination.

16. At bottom, the Office of General Counsel (OGC), from which each of the aforementioned documents originated, has no policy role, but rather, provides legal advice to its clients that constitutes one consideration among many for policymakers. As noted in my prior submissions, “[t]he NSA OGC is the exclusive NSA component for providing legal services to all NSA elements and is led by the General Counsel, who is the NSA’s chief legal officer.” (Supp. NSA Decl., Dkt. No. 79, ¶ 16). While OGC “provides legal advice on a number of different legal matters, . . . the office has no authority to issue final decisions or authoritative statements on NSA policy,” to include those policies referenced in NSA Documents 7, 14-21 and 28. (*Id.*).

**Segregability and Unclassified/FOUO Information in Withholdings Made Pursuant to
FOIA Exemptions 1 and 3**

17. In addition to the aforementioned legal memoranda, NSA withheld in full two Inspector General Reports (NSA Documents 22 and 23), as well as withheld in part a Quarterly Report to the President’s Intelligence Oversight Board (NSA Document 79), pursuant to Exemptions 1 and 3, which were in turn challenged by ACLU. Plaintiffs similarly challenged the withholding in full of NSD Documents 7, 37, 42, 44, and 47. With respect to these materials, the Court stated that Defendants failed to “address in their reply whether they did conduct a line-by-line segregability review on these . . . documents,” instructing Defendants to “conduct such a segregability review . . . or inform the Court that this review has already occurred.” (Mem. at 36).

18. First and foremost, I respectfully direct the Court to Paragraph 84 of my UNCLASSIFIED declaration which states that “[a]ll of these documents have been reviewed for purposes of complying with FOIA’s segregability provision,” adding that “[a]n intensive, line-by-line review of each document was performed.” (NSA Decl., Dkt. No. 64, ¶ 84). Moreover, I explained that with respect to these materials and any information withheld under Exemption 1, even “information that, viewed in isolation, could be considered unclassified, is nonetheless

classified in the context of this case because it can reasonably be expected to reveal (directly or by implication) classified national security information” (*Id.* ¶ 85).

19. Specifically, with respect to NSD Documents 7, 37, 42, 44, and 47, which were also discussed in detail in my CLASSIFIED declaration, I explained in my supplemental UNCLASSIFIED declaration that “these documents concern in their entirety specific classified operations or activities of the Agency that have not been publicly acknowledged and *do not contain any segregable information*,” as the “compliance matters discussed therein are inextricably intertwined with factual descriptions of NSA functions and activities that are both classified and protected from public disclosure by statute.” (Supp. NSA Decl., Dkt. No. 79, ¶ 13 (emphasis added)). Accordingly, after performing a segregability review of these NSD materials containing NSA equities, I “determined that no portion of these documents could reasonably be segregated and released.” (*Id.*).

20. With respect to NSA Document 22 (as well as the aforementioned NSD documents), which are all discussed in my CLASSIFIED declaration (*see, e.g.*, NSA Class. Decl. ¶¶ 7-10), my initial review determined that “[o]ther than the . . . dates and number of pages, no information . . . [could] be released because the very fact of” the intelligence sources and methods implicated “is currently and properly classified.” (NSA Decl., Dkt. No. 64, ¶ 38).

21. Similarly, concerning NSA Document 23, my UNCLASSIFIED declaration explains that NSA fully withheld this OIG Report “concerning particular intelligence activities of the NSA, including the dissemination of communications intelligence to partner agencies,” after determining “that there is no reasonably segregable, non-exempt information in the report.” (*Id.* ¶ 58).

22. By contrast, during its review of NSA Document 79, NSA determined that it could indeed segregate certain information, and accordingly, NSA released UNCLASSIFIED materials

including “publicly acknowledged NSA functions and activities,” while nevertheless “protecting the material that remains classified and/or protected from disclosure by law.” (Supp. NSA Decl., Dkt. No. 79, ¶ 13).

23. As part of its review in conjunction with the Court’s 27 March Opinion, NSA again analyzed these materials for segregability, confirming that there are no reasonably segregable portions of those documents that it withheld in full. At bottom, even where “each and every word” in a withheld document is neither classified, nor protected from disclosure by statute, Courts have recognized that to provide such material “standing in a vacuum would be meaningless,” whereas to provide “sufficient context . . . to make the non-exempt material meaningful, the circumstances warranting the classification of the [document] would be revealed.” *Cf. Am. Civil Liberties Union v. Dep’t of Justice*, No. 15 Civ. 9002 (PKC), --- F. Supp. 3d ----, 2017 WL 213812, at *4 (S.D.N.Y. Jan. 18, 2017). It is clear that the “FOIA does not require redactions and disclosure to this extent.” *Id.* (citation omitted); *accord N.Y. Times Co. & Charlie Savage v. Nat’l Sec. Agency*, 205 F. Supp. 3d 374, 381 (S.D.N.Y. 2016) (“This [segregability] provision [of the FOIA] does not require disclosure of non-exempt material rendered meaningless by surrounding deletions.”).

24. Relatedly, with respect to NSA Documents 22, 23, and 79, as well as NSD Documents 7, 37, 42, 44, and 47, the Court instructed Defendants to review these documents “for improper withholding” under Exemption 1 of “Unclassified/For Official Use Only” or “U/FOUO” material. (Mem. at 37). Further to the Court’s direction, upon another review, NSD Documents 7, 37, and 44 do not contain any U/FOUO information and contain solely classified information. NSD Documents 42 and 47, as well as NSA Documents 22 and 23, do contain a limited amount of U and/or U/FOUO information, as well as classified information. These documents were all withheld in full pursuant to both Exemption 1 and Exemption 3. As described in my supplemental UNCLASSIFIED declaration, with respect NSD Documents 42 and 47, “these documents concern

in their entirety specific classified operations or activities of the Agency that have not been publicly acknowledged and do not contain any segregable information.” (See NSA Suppl. Decl., Dkt. No. 79, ¶ 13). I have reviewed the unclassified materials in these documents and find that all such U or FOUO material is not only “inextricably intertwined with factual descriptions of NSA functions and activities that are both classified and protected from public disclosure by statute,” but also meaningless when segregated. (See *id.*). Similarly, with respect to the aforementioned NSD materials, as well as with respect to NSA Document 22, “any description of the information withheld beyond that given below would reveal information that is currently and properly classified . . . and is protected from release by statute as this information would reveal the intelligence sources, methods, activities, and functions of SIGINT collection and exploitation.” (NSA Decl., Dkt. No. 64, ¶ 26 (emphasis added); see also *id.* ¶¶ 41-44). Finally, my UNCLASSIFIED declaration also addressed NSA Document 23 in detail, explaining how “[a]ny disclosure of the withheld information would reveal NSA’s capabilities and the tradecraft used to carry out its vital communications intelligence mission.” (*Id.* ¶ 61); (see also *id.* ¶ 59 (“I have reviewed NSA’s withholding in full of this document and determined . . . that this decision was correct . . .”))).

25. Additionally, specifically with respect to the U/FOUO material that remains redacted in NSA Document 79, every such withholding was made pursuant to Exemption 3 only, in order to protect from disclosure, *inter alia*, NSA organization, functions, or activities. 50 U.S.C. § 3605. Accordingly, NSA is not improperly asserting Exemption 1 over this redacted material.

Classified Annex to DoD Procedures, NSD Document 94-125

26. Defendants also withheld in part the 1988 Classified Annex to the DoD Procedures under EO 12333, or NSD Bates Number NSD094-125. Plaintiffs advanced the argument that the Government had already officially released some of the withheld material in this document,

prompting an additional review by NSA. (See NSA Supp. Decl., Dkt. No. 79, ¶ 16 n.3). The Court directed Defendants to “inform the Court of the result” of this additional review. (Mem. at 38).

27. By letter dated September 26, 2016, Defendants provided a supplemental release of NSD094-125 to Plaintiffs. That letter explained that Defendants “re-processed this document in an attempt to maximize the disclosure of segregable, non-exempt portions of the document, and further, to ensure consistency with prior releases of the same document.”

CONCLUSION

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed this 14th day of June, 2017, pursuant to 28 U.S.C. § 1746.



Dr. David J. Sherman
Associate Director for Policy and Records,
National Security Agency

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

AMERICAN CIVIL LIBERTIES UNION
and AMERICAN CIVIL LIBERTIES
UNION FOUNDATION,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY,
CENTRAL INTELLIGENCE AGENCY,
DEPARTMENT OF DEFENSE,
DEPARTMENT OF JUSTICE, and
DEPARTMENT OF STATE,

Defendants.

No. 13-CV-9198 (KMW)

DECLARATION OF KEVIN G. TIERNAN

I, Kevin G. Tiernan, declare as follows:

1. I am the Supervisory Records Manager of the Records and Freedom of Information Act (“FOIA”) Unit of the Office of Risk Management and Strategy in the National Security Division (“NSD”) of the United States Department of Justice (“DOJ” or “Department”). NSD is a component of the Department. NSD formally began operations on October 2, 2006, by consolidating the resources of the Department’s Office of Intelligence Policy and Review (“OIPR”)¹ and the Criminal Division’s Counterterrorism Section (“CTS”) and Counterespionage Section (“CES”)². As the Supervisory Records Manager, I supervise NSD’s records management and FOIA personnel. In that capacity, I oversee the processing of all FOIA requests made to NSD and the management of the Division’s records, a large percentage of

¹ OIPR is now known as the Office of Intelligence (“OI”).

² CES is now known as the Counterintelligence and Export Control Section.

NSD's records include information that is properly classified under Executive Order 13526. In addition, I am the Department's liaison to the Interagency Security Classification Appeals Panel ("ISCAP") which reviews appeals of mandatory declassification review requests under Executive Order 13526.

2. In a letter dated May 13, 2013, plaintiffs the American Civil Liberties Union and the American Civil Liberties Union Foundations ("plaintiffs"), requested the following:

- (1) Any records construing or interpreting the authority of the National Security Division ("NSD") under Executive Order 12,333 or any regulations issued thereunder;
- (2) Any records describing the minimization procedures used by the NSD with regard to both intelligence collection and intelligence interception conducted pursuant to the NSD's authority under EO 12,333 or any regulations issued thereunder; and
- (3) Any records describing the standards that must be satisfied for the "collection," "acquisition," or "interception" of communications, as the NSD defines these terms, pursuant to the NSD's authority under EO 12,333 or any regulations issued thereunder.

This request was assigned NSD FOI/PA #13-175.

3. Plaintiffs served their complaint in this lawsuit on the United States Attorney for the Southern District of New York on December 30, 2013.

4. In a letter dated May 14, 2014, NSD informed plaintiffs that Executive Order 12333 governs intelligence collection by intelligence agencies, and that because NSD is not an intelligence agency, it does not collect intelligence. In addition, NSD stated that it has no authority under Executive Order 12333, and, as a result, NSD possessed no responsive records.

5. In a letter dated July 29, 2014, ACLU submitted a new request for the following information:

- (1) Formal regulations or policies relating to any agency's authority under EO 12,333 to undertake "Electronic Surveillance" (as that term is defined

in EO 12,333) that implicates “United States Persons” (as that term is defined in EO 12,333), including regulations or policies relating to the acquisition, retention, dissemination, or use of information or communications to, from, or about United States Persons under such authority.

- (2) Records that officially authorize or modify under EO 12,333 any agency’s use of specific programs, techniques, or types of Electronic Surveillance that implicate United States Persons, including official rules or procedures for the acquisition, retention, dissemination, or use of information or communications to, from, or about United States persons under such authority generally or in the context of particular programs, techniques, or types of Electronic Surveillance.
- (3) Formal legal opinions addressing any agency’s authority under EO 12,333 to undertake specific programs, techniques, or types of Electronic Surveillance that implicates United States Persons, including formal legal opinions relating to the acquisition, retention, dissemination, or use of information or communications to, from, or about United States Persons under such authority generally or in the context of particular programs, techniques, or types of Electronic Surveillance.
- (4) Formal training materials or reference materials (such as handbooks, presentations, or manuals) that expound on or explain how any agency implements its authority under EO 12,333 to undertake Electronic Surveillance that implicates United States Persons, including the acquisition, retention, dissemination, or use of information or communications to, from, or about United States Persons under such authority.
- (5) Formal reports relating to Electronic Surveillance under EO 12,333 implicating United States Persons that contain any meaningful discussion of (1) any agency’s compliance, in undertaking such surveillance, with EO 12,333, its implementing regulations, the Foreign Intelligence Surveillance Act, or the Fourth Amendment; or (2) any agency’s interception, acquisition, scanning, or collection of the communications of United States Persons, whether “incidental” or otherwise, in undertaking such surveillance; and that are or were:
 - (a) Authored by an inspector general or the functional equivalent thereof;
 - (b) Submitted to Congress, the Office of the Director of National Intelligence, the Attorney General, or the Deputy Attorney General;
or
 - (c) Maintained by the office of the Assistant Attorney General for

National Security.

This request was assigned NSD FOI/PA #14-177.

6. On October 31, 2014, ACLU filed an amended complaint, which made the July 29, 2014 request a part of the December 30, 2013 lawsuit.

7. After a series of voluntary disclosures and discussions among the parties, the Government moved for summary judgment, supported by various declarations describing each agency's search for responsive records, and explaining the basis for any withholdings of responsive records. One such declaration (ECF NO. 65) was made on February 26, 2016, by John Bradford Wiegmann, who serves as the Deputy Assistant Attorney General of NSD ("Wiegmann Decl."). As the Wiegmann Declaration explained, NSD's search located 68 responsive records; eight of those records were released in full to plaintiffs, nine were released in part, and the remaining 51 were withheld in full. Plaintiffs indicated that they wished to challenge only 19 of the 68 NSD documents withheld in full, namely NSD 2, 4, 7, 9, 12, 13, 14, 17, 18, 23, 30, 31, 33, 36, 37, 42, 44, 47, and 48. Plaintiffs also challenged the partial withholding of the documents Bates numbered NSD 94-125 and NSD 202-207. These documents were described in an index attached to the Wiegmann Declaration. NSD withheld the documents numbered NSD 2, 4, 7, 9, 12, 13, 14, 17, 18, 23, 30, 31, 33, 36, 37, 42, 44, 47, and 48 in full and NSD 94-125 and NSD 202-207 in part pursuant to FOIA Exemptions 1, 3, and/or 5, as detailed in the Wiegmann Declaration and the index. Mr. Wiegmann also provided a supplemental declaration (ECF No. 80)("Supplemental Wiegmann Decl.") in June 2016 in connection with the Government's reply memorandum and opposition to plaintiffs' cross-motion for partial summary judgment, which provided further information regarding the withheld documents.

8. In a Memorandum Opinion and Order dated March 27, 2017, this Court stated that it could not conclude based on the information provided to date that NSD had conducted an adequate search for documents responsive to plaintiffs' request. This Court also denied the Government's motion for summary judgment to the extent that motion was based on the assertion of FOIA Exemption 5 as to NSD 12, 13, 14, 23, 33, and 49. The same ruling, however, upheld the Government's assertion of FOIA Exemptions 1 and 3 as to those same documents. The Court further invited the Government to submit additional information to also justify NSD's assertion of Exemption 5 as to these documents, as well as to further explain the agency's search. This declaration provides additional information from and on behalf of NSD. Declarants from other agencies will address other issues identified in the Court's order.

NSD's Search for Responsive Records

9. As discussed in the February 26, 2016 and June 8, 2016 Wiegmann Declarations, NSD determined that the most effective way to search for responsive documents was to identify and then direct six attorneys in NSD's OI³ and one attorney in the NSD's Office of Law and Policy,⁴ who have worked on issues concerning electronic surveillance under Executive Order 12333 described in the request, to conduct searches for responsive documents. The six attorneys within NSD's Office of Intelligence consisted of (1) a Counsel to the Assistant Attorney General, (2) the Section Chief of Operations, (3) the Section Chief of Oversight, (4) a Deputy Section Chief of Operations, (5) a second Deputy Section Chief of Operations, and (6) a Unit Chief in the Operations Section. The seventh NSD attorney who searched his files for responsive records

³ NSD's OI ensures that the Intelligence Community agencies have certain legal authorities necessary to conduct intelligence operations, particularly operations involving the Foreign Intelligence Surveillance Act (FISA); exercises oversight over the Intelligence Community's use of FISA authorities; and assists in FISA-related litigation.

⁴ NSD's Law and Policy Office develops and implements Department of Justice policies with regard to intelligence, counterterrorism, and other national security matters and provides legal assistance and advice on matters of national security law.

was the Special Counsel within the Office of Law and Policy. In addition, as explained below, NSD staff conducted a search of historical files that predated the formation of NSD in 2006.

10. NSD searched for responsive records primarily through the aforementioned individuals because, individually and collectively, they possessed the seniority, institutional experience and knowledge, and areas of responsibility that would cover all of NSD's involvement with EO 12333 intelligence issues, and all of NSD's records that would be reasonably likely to contain records responsive to plaintiffs' requests. NSD's relevant records are not kept in a system that can readily be searched electronically using search terms, and they are not widely dispersed within the agency; rather, all pertinent NSD records are maintained in case-specific or issue-specific files maintained by NSD legal personnel, and the individuals whom NSD selected to search were organizationally responsible for and knowledgeable about NSD's activities relating to EO 12333 intelligence, and all records of any such activities. As a result, NSD's search used the best available means to uncover all NSD records responsive to plaintiffs' requests, and no additional search methods are likely to reveal responsive NSD records or record systems that were not searched as a result of the processes that NSD employed through these individuals.

11. Specifically, the Counsel for Intelligence to the Assistant Attorney General was an attorney in NSD from August 2007 (just ten months after NSD was created) to May 2016. During that time, he was an attorney advisor in NSD's Office of Intelligence ("OI") from August 2007 to December 2014 and the Counsel for Intelligence from December 2014 to May 2016. While in OI, he served as an attorney advisor in the Operations Section from August 2007 to approximately October 2008 and in the Oversight Section from October 2008 to December 2014. His duties during his time in Operations and Oversight included oversight of the National

Security Agency (“NSA”). As part of his duties as an attorney advisor in the Oversight Section, he led various aspects of NSD’s oversight program regarding NSA’s use of the Foreign Intelligence Surveillance Act (“FISA”), including but not limited to its implementation of Section 702 of FISA. While the Oversight Section did not oversee Executive Order 12333 activities, Executive Order 12333 authorities and their application were relevant to ensuring that NSA’s activities were carried out consistent with FISA. The Counsel’s job duties when he was an attorney advisor in OI included running the day-to-day operations of NSD’s oversight teams, receiving briefings regarding NSA collection capabilities and authorities, conducting oversight reviews, and investigating potential incidents of non-compliance with FISA authorities. As a result of those duties, the Counsel had access to (and in certain cases, helped create the organizational structure of) the electronic folders that contained virtually all of NSD OI’s oversight records pertaining to NSA.⁵

12. Given the nature of plaintiffs’ request and the manner in which the relevant files are kept, it would not have been effective or efficient for the Counsel for Intelligence to use search terms to try to locate potentially responsive records. Instead, he conducted a manual search through all relevant electronic folders to identify responsive documents. As both a subject matter expert and the creator of many of these oversight folders, he was aware of where materials potentially responsive to this FOIA request would be located. He supplemented this search by also searching through his hard copy files for topics related to Executive Order 12333 collection for potentially responsive documents. These hard copy files were organized in folders that were labeled by project name or subject matter.

⁵ The remaining oversight records were accessible by the Deputy Chief of Operations and the Unit Chief of Operations, both of whom conducted searches for records responsive to this FOIA request, as described below.

13. The Section Chief of Operations also conducted a search for responsive records. He first began working in OIPR in October 2001, and has served as the Chief of OI's Operations Section since April 2010, as well as the Acting Chief from September 2009 to April 2010. As the Section Chief of Operations, he is responsible for overseeing OI's operational work, including the preparation of requests for electronic surveillance and physical search pursuant to FISA. Again, given the nature of plaintiffs' request and the manner in which the relevant files are kept, it would not have been effective or efficient for the Section Chief of Operation to use search terms to try to locate responsive records. Instead, as part of his review, he searched in those portions of his electronic and paper files which he believed would contain potentially responsive materials. As both a subject matter expert and as the creator of his files, he knew where materials responsive to this FOIA request would be located.

14. In addition, OI's Oversight Section Chief also searched for responsive records. The Oversight Section Chief first started working in OIPR in June 2004 as an attorney advisor. He was promoted to Assistant Counsel in March 2005 and became the Oversight Section Chief in 2008. As Oversight Section Chief, he is responsible for overseeing the Intelligence Community's foreign intelligence collection. The Oversight Section Chief reviewed his hard copy and electronic files to identify responsive records in his possession. His electronic records are organized by subject matter, which allowed for ready identification of potentially responsive records. As both a subject matter expert and as the creator of his files, he knew where materials responsive to this FOIA request would be located, and did not use, or need to use, search terms to locate relevant documents.

15. Two Deputy Section Chiefs of Operations also searched for responsive records. The first Deputy Section Chief has been in the office since February 2005. He was an attorney

advisor until 2006, and then became an Associate Counsel from 2006 to 2008. From 2008 to 2010, he served as the Unit Chief for Special Operations and, since 2010, has been a Deputy Section Chief of Operations. The Deputy Section Chief of Operations personally went through his paper and electronic files and searched for relevant projects he had worked on as well as for any Executive Order 12333-related documents in his possession. As both a subject matter expert and as the creator of his files, he knew where materials responsive to this FOIA request would be located, and did not use, or need to use, search terms to locate relevant documents.

16. The second Deputy Section Chief also searched for responsive records. The second Deputy Section Chief started working as an attorney advisor in OIPR in January 2004. He was promoted to Associate Counsel in June 2006 and became a Deputy Section Chief in April 2008. He left the Department in September 2015. The second Deputy Section Chief searched his electronic files and his paper files, and as both a subject matter expert and as the creator of his files, he knew where materials responsive to this FOIA request would be located.

17. The sixth OI attorney who searched for responsive records was the Unit Chief in the Operations Section. He joined OIPR in December 2004 as an Attorney Advisor, was promoted to Deputy Unit Chief in May 2008, and became the Unit Chief of Operations in May 2010, a position he holds to this day. He manually searched his hard copy files and his electronic records. His hard copy records are organized into separate physical folders or binders and are labeled by project name or subject matter. The vast majority of his electronic files are organized into separate electronic folders labeled by project name or subject matter. He reviewed those files manually to locate and identify responsive records. He also has a small number of electronic folders that he uses to store miscellaneous documents, and those folders are labeled in a manner that makes the files' contents easily identifiable. The Unit Chief manually searched

these miscellaneous electronic folders to identify responsive documents. Due to the manner in which the Unit Chief labels his files, he did not rely on search terms or keywords to conduct his searches because doing so would have resulted in an under-inclusive search. Instead, the Unit Chief was able to look at the project names, subject matter, or file names of his paper and electronic files to determine whether a given folder or file contained responsive records.

18. These six OI attorneys were among the most senior attorneys in OI and were in the highest positions of leadership in that office. They had supervisory responsibilities and possessed the most comprehensive institutional knowledge about Executive Order 12333. They oversaw all of the work OI did on matters pertaining to Executive Order 12333, and any additional records possibly located in the files of another OI employee would likely have been duplicated in the files of at least one of these six attorneys. In addition, after these attorneys conducted their initial searches, the results of those searches were amalgamated, and all six of these attorneys met for several hours. They used their collective experience and institutional knowledge to review the potentially responsive documents and to confirm that the searches were comprehensive and produced a complete set of responsive records.

19. Finally, the Special Counsel within the Office of Law and Policy also searched his records. The Special Counsel joined OIPR, a predecessor to NSD, in 1997 as an attorney advisor. Prior to working in the Office of Law and Policy, the Special Counsel worked as a Deputy Counsel in OIPR, and he is among the most knowledgeable attorneys in the Office of Law and Policy on surveillance matters. Because of this, he continues to work on and advise others working on critical surveillance related matters. In addition, the Special Counsel works more on Executive Order 12333-related matters than anyone else in the Office of Law and Policy. The Special Counsel reviewed his hard copy and electronic files, which are organized by

subject matter to search for responsive records. As both a subject matter expert and as the creator of his files, he knew where materials responsive to this FOIA request would be located.

20. There is no other reasonably achievable search method that would be likely to uncover additional responsive records; specifically, other employees' individual files would not be likely to contain responsive records that the senior, supervisory personnel assigned to search would not have either possessed or obtained based on their own expertise about NSD activities and who at NSD worked on what EO 12333-related tasks. Therefore, it is unlikely that any additional responsive records would be located in the files of other employees within NSD.

21. The searches conducted by these senior NSD employees and their additional discussions to ensure comprehensiveness were the primary means that NSD employed to achieve a complete search that would yield all responsive records. In addition to these individuals' searches and consultations, as explained in the Supplemental Wiegmann Declaration, NSD FOIA staff also conducted a search of OIPR's historical policy working files for potentially responsive records that were generated before NSD's formation in 2006. NSD maintained these files as an archive of historic policy and operational documents that formerly was consulted by OIPR attorneys until NSD was established. The goal of this supplemental search was to identify any additional pre-NSD records (if any) on which DOJ and the IC agencies governed by EO 12333 continue to rely as authoritative, but NSD's primary means of identifying records known to NSD about EO 12333 activities was NSD's search by the senior-level individual searches. NSD electronically and manually searched the OIPR archives using the search term "12333 procedures" and evaluated each 'hit' for responsiveness to the request. Together, these searches covered all the systems and types of files that were likely to contain responsive records possessed by each attorney, and NSD FOIA is unaware of other locations or personnel that

would be likely to yield additional responsive information. Due to the nature of the duties, seniority, and institutional knowledge of the senior officials who carried out the search, it is unlikely that any other NSD personnel would have responsive records that at least one of the seven attorneys who conducted searches did not also have, beyond the historical records that were searched separately.

Invocation of Exemption 5 for NSD 12, 13, 14, 23, 33, and 49 and NSA 11 and 12

22. The Wiegmann Declaration stated that FOIA Exemption 5, and specifically the attorney-client and deliberative-process privileges, applied to the “vast majority” of the documents designated NSD 12, 13, 14, 23, 33, and 49, and NSA 11 and 12. In its order, the Court invited NSD to “supplement its submissions with detail about what portions of these documents do, and do not, contain legal advice or deliberative and pre-decisional analysis.”

23. Documents NSD 12, 13, 14, 33, and 49 and NSA 11 and 12 each consist of a number of sub-documents: privileged and deliberative memoranda from an Executive Branch official to another Department of Justice official recommending that s/he take a particular course of action; and non-privileged, non-deliberative documents reflecting the governmental action decisions that occurred after consideration of those recommendations. Document NSD 23, in its entirety, is a privileged and deliberative memorandum from a Department of Justice official to another Department of Justice official recommending that s/he take a particular course of action. NSD asserts Exemption 5 only for the portion of each of those documents that consists of memoranda. I note, however, that all of these documents are classified in their entirety and therefore protected in full from disclosure by FOIA Exemptions 1 and 3, as the Court has already held.

24. Specifically, NSD 12 is 36 pages long, of which the privileged memoranda consist of 14 pages; NSD 13 is 111 pages long, of which the privileged memoranda consist of 46

pages; NSD 14 is 45 pages long, of which the privileged memoranda consist of 32 pages; NSD 23 consists exclusively of a privileged memorandum and is four pages long; NSD 33 is 52 pages long, of which the privileged memoranda consist of 31 pages; NSD 49 is 24 pages long, of which the privileged memoranda consist of 16 pages; NSA 11 is 45 pages long, of which the privileged memoranda consists of 40 pages; and NSA 12 is 87 pages long, of which the privileged memoranda consist of 85 pages.

CONCLUSION

I certify, pursuant to 28 U.S.C. § 1746, under penalty of perjury that the foregoing is true and correct.

Executed this 14th day of June 2017, Washington, DC



KEVIN G. TIERNAN

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

AMERICAN CIVIL LIBERTIES UNION and
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY,
CENTRAL INTELLIGENCE AGENCY,
DEPARTMENT OF DEFENSE,
DEPARTMENT OF JUSTICE, and
DEPARTMENT OF STATE,

Defendants.

No. 13-cv-09198 (KMW)

ECF Case

NOTICE OF APPEAL

NOTICE IS HEREBY GIVEN that the American Civil Liberties Union and the American Civil Liberties Union Foundation, Plaintiffs in the above-named case, hereby appeal to the United States Court of Appeals for the Second Circuit from the final judgment entered in this action on August 22, 2017 (Docket No. 113).

Dated: October 20, 2017

Respectfully submitted,

/s/ Ashley Gorski

Ashley Gorski
Patrick Toomey
American Civil Liberties Union
Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654

agorski@aclu.org

Hannah Bloch-Wehba
David Schulz
Diana Lee (law student intern)
Sebastian Brady (law student intern)
Paulina Perlin (law student intern)
Media Freedom and Information
Access Clinic,
Abrams Institute, Yale Law School
P.O. Box 208215
New Haven, CT 06520
Phone: (212) 850-6103
hannah.bloch-wehba@yale.edu

Counsel for Plaintiffs