GREGORY G. KATSAS
Assistant Attorney General, Civil Division
CARL J. NICHOLS
Principal Deputy Associate Attorney General
JOHN C. O'QUINN
Deputy Assistant Attorney General
DOUGLAS N. LETTER
Terrorism Litigation Counsel
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Special Litigation Counsel
ALEXANDER K. HAAS
PAUL G. FREEBORNE
Trial Attorneys
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW, Rm. 6102
Washington, D.C. 20001
Phone: (202) 514-4782—Fax: (202) 616-8460

Attorneys for the United States

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

IN RE NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION This Document Relates To: ALL CLAIMS AGAINST ELECTRONIC COMMUNICATION SERVICE PROVIDER DEFENDANTS (including *AT&T, MCI/ Verizon, Sprint/Nextel, Cingular Wireless/AT&T Mobility, and BellSouth* Defendants) including in: 06-00672 06-05268 06-06253 06-07934 06-03467 06-05269 06-06295 07-00464 06-03596 06-05340 06-06294 07-01243 06-04221 06-05341 06-06313 07-02029 06-03574 06-05343 06-06388 07-02538 06-05067 06-05452 06-06385 06-05063 06-05485 06-06387 06-05064 06-05576 06-06435 06-05065 06-06222 06-06434 06-05066 06-06224 06-06924 06-05267 06-06254 06-06570; and Master *MCI/Verizon* Compl. (Dkt. 125); Master *Sprint* Compl. (Dkt. 124); Master *BellSouth* Complaint (Dkt. 126); Master *Cingular* Amended Complaint (Dkt. 455)	No. M:06-cv-01791-VRW **UNITED STATES' NOTICE OF MOTION TO DISMISS OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT** Date: December 2, 2008 Time: 10 a.m. Courtroom: 6, 17th Floor Chief Judge Vaughn R. Walker

PLEASE TAKE NOTICE that, on December 2, 2008 at 10:00 a.m. before Chief Judge Vaughn R. Walker, the United States of America will move to dismiss or, in the alternative, for summary judgment as to claims against electronic communication service provider-defendants in the above-referenced proceeding pursuant to Rules 12(b)(1), (b)(6), or 56 of the Federal Rules of Civil Procedure. The grounds for this motion are that these actions should now be promptly dismissed pursuant to Section 201 of Title II of the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. 110-261, 122 Stat. 2467, Title II, § 201 (July 10, 2008) ("FISA Amendments of 2008" or "Act"). The Act established Section 802(a) of the FISA, which provides that a civil action "may not lie or be maintained" against electronic communication services providers alleged to have provided assistance to an element of the intelligence community, and "shall be promptly dismissed" if the Attorney General of the United States certifies that one of several circumstances exist with respect to the alleged assistance. *See* 50 U.S.C. § 1885a(a)(1)-(5). The Attorney General has made the requisite certification under Section 802(a) of the FISA with respect to all claims against the provider-defendants in this proceeding and, accordingly, those claims should now be promptly dismissed.

This motion is supported by the accompanying: (i) Memorandum of Points and Authorities in Support of the United States Motion to Dismiss or for Summary Judgment; (ii) the Public Certification of the Attorney General of the United States authorized by Section 802(a) of the Act, 50 U.S.C. § 1885a(a); (iii) the Classified Certification of the Attorney General of the United States submitted for the Court's *in camera, ex parte* as expressly authorized by Section 802(c) of the FISA, 50 U.S.C. § 1885a(c); and (iv) any "supplemental materials" submitted by the Attorney General with his classified certification (if any), pursuant to Section 802(b)(2) of the FISA, 50 U.S.C. § 1885a(b)(2).

Dated: September 19, 2008

Respectfully Submitted,

GREGORY G. KATSAS
Assistant Attorney General, Civil Division

CARL J. NICHOLS
Principal Deputy Associate Attorney General

JOHN C. O'QUINN
Deputy Assistant Attorney General

DOUGLAS N. LETTER
Terrorism Litigation Counsel

JOSEPH H. HUNT
Director, Federal Programs Branch

s/ Anthony J. Coppolino
ANTHONY J. COPPOLINO
Special Litigation Counsel

s/ Alexander K. Haas
ALEXANDER K. HAAS

s/ Paul G. Freeborne
PAUL G. FREEBORNE

Trial Attorneys
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW, Rm. 6102
Washington, D.C. 20001
Phone: (202) 514-4782—Fax: (202) 616-8460
Email: tony.coppolino@usdoj.gov

Attorneys for the United States

GREGORY G. KATSAS
Assistant Attorney General, Civil Division
CARL J. NICHOLS
Principal Deputy Associate Attorney General
JOHN C. O'QUINN
Deputy Assistant Attorney General
DOUGLAS N. LETTER
Terrorism Litigation Counsel
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Special Litigation Counsel
ALEXANDER K. HAAS
PAUL G. FREEBORNE
Trial Attorneys
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW, Rm. 6102
Washington, D.C. 20001
Phone: (202) 514-4782—Fax: (202) 616-8460

Attorneys for the United States

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

IN RE NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION This Document Relates To: ALL CLAIMS AGAINST ELECTRONIC COMMUNICATION SERVICE PROVIDER DEFENDANTS (including *AT&T, MCI/ Verizon, Sprint/Nextel, Cingular Wireless/AT&T Mobility, and BellSouth* Defendants) including in: 06-00672 06-05268 06-06253 06-07934 06-03467 06-05269 06-06295 07-00464 06-03596 06-05340 06-06294 07-01243 06-04221 06-05341 06-06313 07-02029 06-03574 06-05343 06-06388 07-02538 06-05067 06-05452 06-06385 06-05063 06-05485 06-06387 06-05064 06-05576 06-06435 06-05065 06-06222 06-06434 06-05066 06-06224 06-06924 06-05267 06-06254 06-06570; and Master *MCI/Verizon* Compl. (Dkt. 125); Master *Sprint* Compl. (Dkt. 124); Master *BellSouth* Complaint (Dkt. 126); Master Cingular Amended Complaint (Dkt. 455)	No. M:06-cv-01791-VRW **MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF UNITED STATES' MOTION TO DISMISS OR FOR SUMMARY JUDGMENT** Date: December 2, 2008 Time: 10 a.m Courtroom: 6, 17th Floor Chief Judge Vaughn R. Walker

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES **PAGE(S)**

STATUTES

LEGISLATIVE HISTORY

INTRODUCTION

On July 10, 2008, Congress passed the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. 110-261, 122 Stat. 2467, Title II, § 201 (July 10, 2008) ("FISA Act Amendments of 2008" or "Act"). A critical and central component of the Act is the enactment of Section 802(a) of the FISA, *see* 50 U.S.C. § 1885a(a), which provides that a civil action "may not lie or be maintained" against any person, including electronic communication services providers, for providing assistance to an element of the intelligence community, and "shall be promptly dismissed" if the Attorney General certifies that one of several possible circumstances exist, including that the provider did not provide the alleged assistance, *see id.* § 1885a(a)(5); that the provider assisted the Government subject to an order of the Foreign Intelligence Surveillance Court ("FISC") or other certifications or directives authorized by statute, *see id.* § 1885a(a)(1)-(3); or that the alleged assistance was in connection with an intelligence activity involving communications authorized by the President after the terrorist attacks of September 11, 2001, and ending on January 17, 2001, and was designed to detect or prevent a further terrorist attack on the United States, and was the subject of written requests to a provider indicating that the activity was authorized by the President and had been determined to be lawful. *See id.* § 1885a(a)(4).

These provisions of the Act reflect Congress' fundamental policy judgment that burdensome litigation should not proceed against providers that may have assisted the Government in unique historical circumstances after 9/11 to detect and prevent another catastrophic terrorist attack on the United States and, indeed, that such litigation risks serious harm to national security. Following extensive oversight of the Terrorist Surveillance Program ("TSP") authorized by the President after 9/11, the Senate Select Committee on Intelligence ("SSCI") concluded that "electronic surveillance for law enforcement and intelligence purposes depends in great part on the cooperation of the private companies that operate the Nation's telecommunication system," *see* S. Rep. 110-209 (2007), accompanying S. 2248, Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2007, Senate Select Committee on

Intelligence ("SSCI Report") (Exhibit 1 hereto), at 9, and that, if litigation is allowed to proceed against telecommunication companies alleged to have assisted in such activities, "the private sector might be unwilling to cooperate with lawful Government requests in the future," and the "possible reduction in intelligence that might result from this delay is simply unacceptable for the safety of our Nation." *Id.* at 10 (emphasis added). Accordingly, the special procedures established under the Act for obtaining review and, where the Act is satisfied, prompt dismissal of such litigation, is vital to the public interest.

The Act establishes procedures that permit the Attorney General to demonstrate that the requirements of the Act have been met without the disclosure of information that would harm national security, including intelligence sources and methods. Congress specifically authorized the Attorney General to submit the basis for his certification as to particular provider-defendants solely for *in camera*, *ex parte* review when the Attorney General finds that this is necessary to protect national security. *See* 50 U.S.C. 1885a(c)(1). Indeed, the Act's legislative history makes clear that the identity of electronic communication service providers from which assistance was sought, and any activities in which the Government was engaged or in which providers assisted, or the details regarding any such assistance, must not be disclosed in applying the procedures established under the Act.

As set forth below, plaintiffs generally allege that, following the terrorist attacks of September 11, 2001, the provider-defendants unlawfully assisted the Government in two ways: (1) by facilitating an alleged "dragnet" collection of the content of millions of domestic and international telephone and Internet communications by the Government, and (2) by allegedly making available to the Government records concerning subscriber telephone and Internet communications—both without judicial authorization or otherwise not in compliance with law. Plaintiffs' claims are plainly encompassed within the Act's provisions. *See* 50 U.S.C. § 1885(1) (defining alleged "assistance" by provider-defendants subject to statutory protection).

Accordingly, the Government submits herewith, as expressly authorized by Section 802(a), both a public certification from Attorney General Michael B. Mukasey that all of the

claims in the civil actions pending in this proceeding against the provider-defendants fall within at least one of the five circumstances set forth in the Act, *see* 50 U.S.C. § 1885a(a)(1)-(5), and a classified certification that sets forth the basis for his certification as to particular provider-defendants. *See* Public Certification of the Attorney General of the United States (hereafter Public Certification); *see also* Notice of Lodging *In Camera, Ex Parte* Certification of the Attorney General of the United States. Section 802(b)(1) of the FISA provides that this certification "shall be given effect" unless the Court finds that it "is not supported by substantial evidence provided to the court pursuant to this section." *See* 50 U.S.C. § 1885a(b)(1). As set forth below, the Attorney General's certification complies with all requirements of the Act and is supported by substantial evidence. Accordingly, the Court should promptly dismiss the claims in this proceeding against electronic communication service providers.[1/]

BACKGROUND

A. Claims Against Electronic Communication Service Providers.

As the Court is aware, cases against electronic communication service providers first arose after media reports in December 2005 alleged that the Government had been undertaking certain intelligence activities after the 9/11 attacks. As detailed below, plaintiffs allege that, without judicial authorization and in violation of law, the provider-defendants have assisted the

---

[1] Section 803 of the FISA, as also added by the FISA Act of 2008, expressly preempts the authority of any State, *see* 50 U.S.C. § 1885(9) (defining "State"), to conduct an investigation into any assistance allegedly furnished to the intelligence community by electronic communication service providers, or to require information about such alleged assistance, or from imposing any sanction on the provider for such alleged assistance, or from commencing a civil action against a provider to enforce requirements to disclose information concerning such alleged assistance. *See* 50 U.S.C. § 1885b. Section 803 also authorizes suit by the United States to enforce these statutory preemption provisions, and provides for district court jurisdiction to review such suits. *See id*. Accordingly, the Act precludes the State investigations at issue in the following cases pending in this MDL proceeding: *United States v. Gaw* (07-01242); *United States v. Palermino* (07-01326); *United States v. O'Donnell* (07-01324); *United States v. Maine* (07-01323); *United States v. Volz* (07-01396); *Clayton v. ATT* (07-01187). The disposition of these cases under the Act will be addressed by separate motion. This motion also does not concern pending actions brought solely against Government defendants: *Al-Haramain et al. v. Bush, et al.* (07-00109); *Center for Constitutional Rights et al. v. Bush, et al.* (07-1115); *Shubert et al. v. Bush, et al.* (07-00693); and *Guzzi v. Bush, et al.* (06-06225).

Government with: (1) an alleged "dragnet" on the collection of the content of communications of millions of Americans; and (2) the alleged collection of records concerning the plaintiffs' telephone and electronic communications.

The first such suit, *Hepting et al. v. AT&T et al.* (06-00672), alleges that AT&T was assisting the Government, without court authorization, in both the interception of "vast quantities of American's telephone and Internet communications," and the collection of detailed communications records about millions of customers. *See Hepting* First Amended Complaint ("FAC") ¶¶ 2-6, 41; *see also Hepting et al. v. AT&T et al.*, 439 F. Supp. 2d 974, 996 (N.D. Cal. 2006) (summarizing claims); *see also id*. at 1001, 1005, 1010 (plaintiffs allege "dragnet" that sweeps in the communication content and records of all or substantially all AT&T customers). A second group of more than forty lawsuits arose after media reports in May 2006 alleged that telecommunications carriers were providing telephone call records to the NSA. *See Hepting*, 439 F. Supp. 2d at 988 (citing Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA Today, May 11, 2006). Thereafter, the Judicial Panel on Multi-district Litigation ordered the transfer of all pending cases to this Court. *See* Dkt. 1 (06-cv-1791-VRW). After initial case management proceedings, the Court directed the filing of consolidated complaints setting forth claims against particular provider-defendants, including four consolidated complaints brought against: (i) *MCI/Verizon* Defendants (Dkt. 125); (ii) *Sprint/Nextel* Defendants (Dkt. 124); (iii) *BellSouth* Defendants (Dkt. 126); and (iv) *Cingular Wireless* (*AT&T Mobility*) Defendants (Dkts. 121, 455).[2/]

---

[2] All of the defendants in one of the five Master Consolidated Complaints, *see* Dkt. 123 (naming T-Mobile, Comcast Telecommunications, McLeod USA Telecommunications Services, and Transworld Network Corp.), have been dismissed by stipulation. *See* Dkts. 162, 164, 184, 185. Certain defendants named in other complaints have also been dismissed. *See* Dkt. 230 (dismissing Cellco Partnership dba Verizon Wireless; NYNEX Corp.; GTE Wireless Inc.; GTE Wireless of the South, Inc.; NYNEX PCS Inc.; Verizon Wireless of the East LP; Verizon Internet Services Inc.; Bell Atlantic Entertainment and Information Services Group; Verizon Internet Solutions Inc.; Verizon Technology Corp; Verizon Advanced Data, Inc.); Dkt. 169 (dismissing Bright House Networks LLC); Dkt. 170 (dismissing Charter Communications LLC); Dkt. 85 (dismissing TDS Communications Solutions, Inc.); Dkt. 235 (dismissing Embarq Corporation). In addition, one action that had been pending in this proceeding—*Electron Tubes*

As in *Hepting*, plaintiffs in the consolidated complaints allege that the provider-defendants participated "in an illegal federal government program to intercept and analyze vast quantities of American's telephones and electronic communications and records." *See Verizon* Compl. ¶ 3; *Sprint* Compl. ¶ 3; *BellSouth* Compl. ¶ 3; *Cingular* Compl. ¶ 3; *see also Hepting* FAC ¶¶ 2-3. Plaintiffs rely on statements made by the President, the Attorney General, and the Director of National Intelligence in December 2005 concerning what later was called the "Terrorist Surveillance Program" ("TSP"), under which the President authorized the National Security Agency ("NSA") "to intercept the international communications of people with known links to Al Qaeda and related terrorist organizations." *See Hepting*, 439 F. Supp. 2d at 986-87; *see also Hepting* FAC ¶ 32; *Verizon* Compl. ¶ 139-41; *Sprint* Compl. ¶ 19-21; *BellSouth* Compl. ¶ 39-41; *Cingular* Compl. ¶ 28-30. But, as this Court has noted, plaintiffs "allege a surveillance program of far greater scope than the publicly disclosed 'terrorist surveillance program.'" *Hepting*, 439 F. Supp. 2d at 994. Specifically, plaintiffs allege that the NSA, with the assistance of the provider-defendants, has intercepted "millions of communications made or received by people inside the United States" and use "powerful computers to scan their contents for particular names, numbers, words, or phrases." *See Hepting* FAC ¶ 39; *Verizon* Compl. ¶ 165; *Sprint* Compl. ¶ 44; *BellSouth* Compl. ¶ 64; *Cingular* Compl. ¶ 53. And plaintiffs separately allege that the provider defendants have provided the Government with access to records about their telephone and electronic communications. *See Hepting* FAC ¶¶ 51-63; *Verizon* Compl. ¶¶ 168-71, 174-75; *Sprint* Compl. ¶¶ 48-50, 53-54; *BellSouth* Compl. ¶¶ 68-70, 73-74; *Cingular* Compl. ¶¶ 57-59, 62-63.

Plaintiffs allege that these activities were undertaken without judicial authorization, and seek declaratory and injunctive relief as well as damages based on alleged violations of the First and Fourth Amendments and other federal and state statutory provisions. *See* Hepting FAC ¶¶ 2; 81, 83, 90-149; *Verizon* Compl. ¶ 177, 201-89; *Sprint* Compl. ¶ 56, 72-141; *BellSouth* Compl.

Inc. v. Verizon Communications, et al. (06-cv-6433-VRW)—has been dismissed. *See* Dkt. 178. As a result, the Attorney General's Certification and this motion need not address these dismissed parties or actions.

¶ 76, 101-216; *Cingular* Compl. ¶ 65, 90-321.

B. Summary of Procedural History

On May 13, 2006, the United States moved to intervene in *Hepting* and filed a motion to dismiss or for summary judgment based on the state secrets privilege and related statutory privileges. *See* Dkts. 122-125 (06-cv-672); *see also Hepting*, 439 F. Supp. 2d at 979. The Government supported its assertion of privilege with public and classified declarations (for *in camera, ex parte* review) by the Director of National Intelligence and the Director of the National Security Agency. The Court later denied both motions but certified its decision for interlocutory appeal, *see Hepting*, 439 F. Supp. 2d at 1010, and the United States Court of Appeals for the Ninth Circuit granted the Government's and AT&T's petition for interlocutory review. *See* Dkt. 341 (06-cv-672).

In the meantime, actions brought against the *AT&T* Defendants, *Sprint* Defendants, and *Cingular Wireless/AT&T Mobility* Defendants were stayed by stipulation pending disposition of the appeal in *Hepting*. *See* Dkts. 172, 163, 177, 199. Actions against the *MCI/Verizon* Defendants were not stayed, and the Government intervened in those cases and filed a motion to dismiss or for summary judgment again based on the state secrets privilege. *See* Dkts. 253-57. Actions against the *BellSouth* Defendants were stayed pending disposition of the motions filed in the *MCI/Verizon* cases, *see* Dkt. 209, and those motions were terminated by the Court without decision on March 31, 2008, *see* Dkt. 438.

By Order dated August 21, 2008, the Ninth Circuit remanded the *Hepting* appeal in light of the enactment of the FISA Act Amendments of 2008.

C. FISA Act Amendments of 2008

The FISA Act Amendments of 2008 were the result of extensive deliberations between Congress and the Executive Branch over the need to modernize and streamline provisions of the FISA, and to address the serious burdens and potential harm to national security of lawsuits against electronic communication service providers alleged to have assisted the Government with intelligence activities after the 9/11 attacks.

Title I of the Act, which is not at issue in the pending claims against provider-defendants, establishes new procedures to facilitate the targeting of communications of persons reasonably believed to be outside the United States in order to acquire foreign intelligence information. *See* 50 U.S.C. §§ 1881a-1881g. Title II of the Act establishes Section 802(a) of the FISA, which provides that civil actions brought against persons, including electronic communication services providers, alleged to have furnished assistance to an element of the intelligence community shall be promptly dismissed if the Attorney General certifies to the district court of the United States in which such action is pending that one of several circumstances exist with respect to the alleged assistance. *See* 50 U.S.C. § 1885a(a).[3/] Section 802(a) sets forth five separate grounds warranting dismissal of such actions, including where any assistance was provided pursuant to: (1) an order of the Foreign Intelligence Surveillance Court directing the provider to furnish such assistance; or (2) a certification in writing from the Attorney General to the provider under 18 U.S.C. § 2511(2)(a)(ii)(B) or 18 U.S.C. § 2709(b); or (3) a directive from the Attorney General or Director of National Intelligence that the provider furnish assistance authorized by the Protect America Act of 2007 or the FISA Act of 2008. *See* 50 U.S.C. § 1885a(a)(1)-(3).

Section 802(a) also bars a cause of action in any "covered civil action" where the assistance alleged to have been provided by an electronic communication service provider was—

> (A) in connection with an intelligence activity involving communications that was—
>
> > (i) authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007; and
> >
> > (ii) designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States; and

---

[3] The definition of "person" under the Act includes an "electronic communication service provider," which is a telecommunications carrier as defined in 47 U.S.C. § 153; a provider of electronic communication service as defined in 18 U.S.C. § 2510; a provider of a remote computing service as defined in 18 U.S.C. § 2711; any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; a parent, subsidiary, affiliate, successor, or assignee of the foregoing entities; or an officer, employee, or agent thereof. *See* 50 U.S.C. § 1885(6), (8). It is indisputable that the provider-defendants in this proceeding qualify as "persons" and "electronic communication service providers" for purposes of the Act.

> (B) the subject of a written request or directive, or a series of written requests or directives, from the Attorney General or the head of an element of the intelligence community (or the deputy of such person) to the electronic communication service provider indicating that the activity was—
>
> (i) authorized by the President; and
>
> (ii) determined to be lawful[.]

50 U.S.C. § 1885a(a)(4).[4/]

Finally, Section 802(a) also provides that a cause of action may not lie against a provider-defendant where the Attorney General certifies that the provider "did not provide the alleged assistance." 50 U.S.C. § 1885a(a)(5).

A certification by the Attorney General that at least one of these five conditions has been met "shall be given effect unless the court finds that such certification is not supported by substantial evidence provided to the court pursuant to this section." 50 U.S.C. § 1885a(b)(1). Section 802 provides further that, in its review of a certification under subsection (a), the court may examine certain "supplemental materials" that track the various grounds for the certification in Section 802(a), namely any court order (§ 802(a)(1)); an Attorney General certification under 18 U.S.C. § 2511(2)(a)(ii)(b) (§ 802(a)(2)); and any directive or written request seeking assistance (§ 802(a)(3) or (4)). *See id.* § 1885a(b)(2).

Section 802 of the FISA also establishes special procedures for implementing this provision without the disclosure of information that would harm national security. Specifically,

---

[4] The Act defines several key terms referenced in this provision. A "covered civil action" to which Section 802(a)(4) applies is defined to mean a civil action filed in a Federal or State court that—

> (A) alleges that an electronic communication service provider furnished assistance to an element of the intelligence community; and
>
> (B) seeks monetary or other relief from the electronic communication service provider related to the provision of such assistance.

See 50 U.S.C. § 1885(5). "Assistance" means "the provision of, or the provision of access to, information (including communication contents, communications records, or other information relating to a customer or communication), facilities, or another form of assistance." *See id.* § 1885(1).

Section 802(c) provides that, if the Attorney General files a declaration under 28 U.S.C. §1746 attesting that disclosure of a certification or any accompanying supplemental materials would harm the national security of the United States, the court shall review such certification and supplemental materials *in camera* and *ex parte*, and may not in any public order following such review disclose which of the five alternatives under Section 802(a) form the basis for the certification. *See* 50 U.S.C. § 1885a(c)(1). To further protect national security interests, Section 802(d) also provides that "[t]o the extent that classified information is relevant to the proceeding or would be revealed in the determination of an issue, the court shall review such information *in camera* and *ex parte*, and shall issue any part of the court's written order that would reveal classified information *in camera* and *ex parte* and maintain such part under seal." 50 U.S.C. § 1885a(d).

The relevant legislative history to the Act[5/] sets forth the background and purpose of Section 802 of the FISA. *See* S. Rep. 110-209 at 7-12 (Exhibit 1). Following extensive oversight of the TSP,[6/] the Senate Select Committee on Intelligence—the committee that originated legislation that ultimately became the FISA Amendments Act of 2008—concluded that "there is a strong national interest in addressing the extent to which the burden of litigation over the legality of surveillance should fall on private parties." *Id.* at 8. In reaching this conclusion, the SSCI found that, beginning soon after September 11, 2001, the Executive Branch

---

[5] No formal conference was convened to resolve the differences between the original House and Senate versions of the Act (S. 2248 and H.R. 3773). Instead, following an agreement reached without a formal conference, the House passed a new bill, H.R. 6304, which contains "a complete compromise of the differences between the House and Senate versions." *See* 154 Cong. Rec. S6097, 6129 (daily ed. June 25, 2008) (Section-by-Section Analysis and Explanation of H.R. 6304, the FISA Act Amendments of 2008). H.R. 6304 is a "direct descendant" of the original House and Senate bills, and "the legislative history of those measures constitutes the legislative history of H.R. 6304." *Id.* (A true and correct copy of the Section-by-Section Analysis is submitted herewith as Exhibit No. 2).

[6] The SSCI Report describes the committee's extensive oversight of the President's program, including seven hearings, classified briefings, answers to written questions, and formal testimony from companies alleged to have participated in the program. *Id.* at 2. The committee also reviewed correspondence that was provided to private sector entities concerning the President's program, as well as the presidential authorizations that supported them. *See id.*

provided written requests or directives to certain electronic communication service providers to obtain their assistance with communications intelligence activities that had been authorized by the President. *See id.* at 9. The SSCI Report indicates that the letters were furnished at regular intervals to providers who assisted the Government, stated that the activities had been authorized by the President, and provided that the activities had been determined to be lawful by the Attorney General, except for one letter that covered a period of less than sixty days. *Id.*[7/]

The SSCI made no assessment of the legality of the President's program, but simply recognized that, at a unique moment in history, immediately after the nation had suffered its worst terrorist attack, private sector entities accepted written representations from high-level Government officials that assistance was needed to prevent another attack, and had been authorized by the President and determined to be lawful. *See* S. Rep. 110-209 at 9-10. The SSCI Report noted in particular the "extraordinary nature of the time period" following the 9/11 attacks, and recognized that the Terrorist Surveillance Program was "an early warning system . . . to detect and prevent the next terrorist attack . . . a program with a military nature that requires speed and agility." *See id.* at 4. The report also recognized that the TSP was authorized amid the backdrop of the 9/11 attacks— indeed, that at the very time the President was authorizing TSP, Congress had authorized the President "'to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided" in the attacks. *Id.* (quoting Authorization for Use of Military Force, Pub. L. 107-40, 115 Stat. 224, Section 2(a) (2001)). In addition, the SSCI found that there was "a continuing and immediate threat of further attacks on the United States" in October 2001 when the TSP was authorized, and that concerns about a further terrorist attack "have persisted to the present day"— citing the United Kingdom aviation plot of August 2006 and the bombing plots in Germany in 2007. *Id.* at 5.

The SSCI Report also makes clear, however, that Section 802(a)(4)—which provides for

---

[7] That letter, which like all the others stated that the activities had been authorized by the President, stated that the activities had been determined to be lawful by the Counsel to the President. *See id.*

dismissal of certain "covered civil actions" that concern assistance furnished by providers subject to written requests after the 9/11 attacks—is restricted to "discrete past activities" and is a "one-time response to an unparalleled national experience in the midst of which representations were made that assistance to the Government was authorized and lawful." *See* S. Rep. 110-209 at 10-11. Under these circumstances, the SSCI found that providers should not be burdened by litigation based on allegations that they assisted the Government at this critical time. This conclusion is buttressed by significant national security considerations—notably that the cooperation of telecommunication companies is essential to intelligence and law enforcement matters, and that the possible reduction in that cooperation caused by protracted litigation against these providers "is simply unacceptable for the safety of our Nation." *Id.* at 10.

The SSCI Report indicates that the Act is meant to apply to the numerous lawsuits pending in this Court. The report recounts that the lawsuits pending in this proceeding allege that electronic communication service providers assisted the federal government in intercepting phone and Internet communications of people within the United States, and that some of the lawsuits seek to enjoin the providers from furnishing records to the intelligence community, while others seek damages for alleged statutory and constitutional violations from the alleged provision of records to the intelligence community. *See* S. Rep. 110-209 at 7. The report also states that the Government intervened and sought dismissal of these suits based on the state secrets privilege, that "the future outcome of this litigation is uncertain," and that "[e]ven if these suits are ultimately dismissed on state secrets or other grounds, litigation is likely to be protracted. . . ." *Id.*

Section 802 of the FISA—the culmination of the Legislative and Executive Branches' careful deliberations on the matter—was enacted to avoid the need to consider the Government's state secrets privilege assertion, but in a manner that does not disclose classified national security information identifying any providers that may have assisted the Government or information concerning alleged activities. The SSCI found that the "details of the President's program are highly classified" and that, as with other intelligence matters, the identities of persons or entities

who provide assistance to the U.S. Government are protected as vital sources and methods of intelligence." *See* S. Rep. 110-209 at 9. Notably, the SSCI expressly stated that "[i]t would be inappropriate to disclose the names of the electronic communication service providers from which assistance was sought, the activities in which the Government was engaged or in which providers assisted, or the details regarding any such assistance." *Id*.; *see also id*. ("identities of persons or entities who provide assistance to the intelligence community are properly protected as sources and methods of intelligence"). Thus, Section 802(a) is designed to protect information that is also subject to the Government's privilege assertions in this proceeding, but authorizes judicial review to determine, through special *ex parte, in camera* proceedings, under a deferential standard of review, if particular facts and circumstances exist with respect to alleged assistance by the provider-defendants that would warrant dismissal under the Act.[8/]

As set forth below, and in the Attorney General's classified certification submitted for *in camera, ex parte* review, the Attorney General has certified that at least one of the circumstances set forth in Section 802(a) have been met with respect to all claims in these proceedings against the provider-defendants, *see generally*, Public Certification of the Attorney General of the United States, and the pending actions against these defendants should therefore be dismissed.

ARGUMENT

I. THE ATTORNEY GENERAL HAS CERTIFIED THAT THE CLAIMS AGAINST THE PROVIDER-DEFENDANTS IN THESE PROCEEDINGS FALL WITHIN AT LEAST ONE OF THE PROVISIONS OF SECTION 802(a) OF THE FISA.

The Attorney General's certification addresses whether the provider-defendants furnished assistance to the Government in connection with plaintiffs' alleged content dragnet and the alleged provision of communication records to the Government. To the extent it may be at issue, the Attorney General's certification also addresses whether the provider-defendants furnished assistance in connection with the Terrorist Surveillance Program. The plaintiffs in these

[8] At the same time, the Act expressly preserves and does not waive or preempt the Government's prior state secrets privilege assertion, *see* 50 U.S.C. § 1885a(h) ("Nothing in this section shall be construed to limit any otherwise applicable immunity, privilege, or defense under any other provision of law").

proceedings have clearly alleged that the provider-defendants provided "assistance" to the Government as defined in the Act, which includes the provision of, or the provision of access to, information, including communication contents and communications records, *see* 50 U.S.C. § 1885(1), and the Attorney General's certification, including his classified certification, indicates that plaintiffs' claims are subject to dismissal based on at least one of the five grounds set forth in Section 802(a)(1)-(5), *see* 50 U.S.C. § 1885a(a)(1)-(5).

A. *Content Dragnet Allegations*: First, as noted above, the plaintiffs have alleged a content collection program of "far greater scope" than the TSP, in which the President authorized the NSA to intercept certain "one-end" international communications to or from the United States that the Government reasonably believed involved a member of agent of al Qaeda or affiliated terrorist organization. *See* Public Certification, ¶ 6; *see also Hepting*, 439 F. Supp. 2d at 994. While confirming the existence of the TSP, the Government has previously denied the existence of the alleged "dragnet" collection on the content of plaintiffs' communications. *See id*. at 996; *see also* Public Declaration of Lt. Gen. Keith Alexander, Director of the National Security Agency, in the *Verizon/MCI* Actions (Dkt. 254) ¶ 17. Accordingly, the Attorney General has certified on the public record that, because there was no such alleged content-dragnet, no provider participated in that alleged activity, and each of the provider-defendants is entitled to statutory protection with respect to claims based upon this allegation pursuant to Section 802(a)5) of the FISA (50 U.S.C. § 1885a(a)(5)). *See* Public Certification ¶ 6. Because information about alleged NSA activities that would be necessary to disprove plaintiffs' content dragnet allegations cannot be disclosed without causing exceptional harm to national security, the basis for the Attorney General's certification concerning the alleged content dragnet is set forth in his classified certification submitted *in camera*, *ex parte* review. *See* Public Certification ¶ 6; *see also* Alexander *Verizon* Declaration ¶ 17.

B. *Terrorist Surveillance Program*: The Attorney General's certification also addresses whether or not any provider-defendant assisted the NSA with the publicly acknowledged TSP. Although the plaintiffs do not appear to directly challenge that activity, any allegation in these

proceedings against a provider-defendant that may encompass TSP assistance is covered by the Attorney General's certification. With respect to any TSP assistance, the Attorney General has certified that the provider-defendants are entitled to statutory protection based on at least one of the provisions contained in Section 802(a)(1) through (5) of the Act, which includes the possibility that a provider-defendant did not provide any assistance, *see* 50 U.S.C. § 1885a(a)(1)-(5). *See* Public Certification ¶ 7. The Attorney General has also attested, pursuant to Section 802(c)(1) of the Act, 50 U.S.C. § 1885a(c)(1), that disclosure of the basis for his certification with respect to whether particular provider-defendants assisted with the TSP would cause exceptional harm to national security and, therefore, is set forth in his classified certification submitted for *ex parte, in camera* review. *See id.* ¶ 7.

C. *Communication Records Allegations*: Finally, with respect to plaintiffs' allegations concerning the collection of telephone and electronic communication records, the Attorney General has also certified that the provider-defendants are entitled to statutory protection based on at least one of the provisions contained in Section 802(a)(1) through (5) of the Act, which includes the possibility that a provider-defendant did not provide any assistance, *see* 50 U.S.C. § 1885a(a)(1)-(5). Public Certification ¶ 8. Because the existence of this alleged activity or any such assistance by the provider-defendants has not been confirmed or denied by the Government, *see Hepting*, 439 F. Supp. 2d at 997, the Attorney General has again attested, pursuant to Section 802(c)(1) of the Act, 50 U.S.C. § 1885a(c)(1), that disclosure of the basis for his certification with respect to the communication records allegations would cause exceptional harm to national security and, therefore, is set forth in his classified certification submitted for *ex parte, in camera* review. *See id.* ¶ 8.

II. THE ATTORNEY GENERAL'S CERTIFICATION IS SUPPORTED BY SUBSTANTIAL EVIDENCE.

Section 802(b) of the FISA provides that the Attorney General's certification "shall be given effect unless the court finds that such certification is not supported by substantial evidence provided to the court[.]" 50 U.S.C. § 1885a(b)(1). The "substantial evidence" standard of review is well-established in law and is "highly deferential[.]" *Pal v. INS*, 204 F.3d 935, 937 n.2

(9th Cir. 2000). "Substantial evidence is such relevant evidence as a reasonable mind might, upon consideration of the entire record, accept as adequate to support a conclusion." *McCarthy v. Apfel*, 221 F.3d 1119, 1125 (9th Cir. 2000) (citing *Richardson v. Perales*, 402 U.S. 389, 401 (1971)). Such review is not *de novo*—that is, under this standard of review, "[i]t is not for the court to strike down conclusions that are reasonably drawn from the evidence and findings in the case" or "to substitute its own conclusions for those which the [Attorney General] had fairly drawn from such findings." *Illinois Cent. R. Co. v. Norfolk & W. Ry. Co.*, 385 U.S. 57, 69 (1966) (citations omitted).

The Attorney General's certification covers discrete factual findings: whether a provider-defendant provided alleged assistance or not; whether, if assistance was provided, the provider-defendant acted subject to an order, certification, directive, or written request that satisfies one of the provisions of Section 802(a). *See* 50 U.S.C. § 1885a(a)(1)-(5). Thus, the narrow issue presented by this motion is whether information submitted to the Court reasonably supports the conclusion that one of these specific factual circumstances exists. The Attorney General has set forth these facts in his certification submitted for *in camera, ex parte* review, and a review of that certification, as well as any supplemental materials provided (if any), makes clear that the certification is amply supported by substantial evidence.

III. THE ATTORNEY GENERAL HAS PROPERLY DETERMINED THAT THE PARTICULAR BASIS FOR HIS CERTIFICATION CANNOT BE DISCLOSED.

Finally, the Attorney General has properly utilized the procedure set forth in Section 802(c) of the Act and determined that disclosure of the basis for his certification with respect to the provider-defendants would cause exceptional harm to national security. *See* Public Certification ¶ 9. Consistent with the Government's prior state secrets privilege assertion, the Act is based on a recognition by Congress that the identities of persons or entities who provide assistance to the intelligence community are properly protected as sources and methods of intelligence, along with the information concerning any alleged activities in which the providers are alleged to have assisted. *See* S. Rep. 110-209 at 9. The special procedures in Section 802(a) permit *in camera, ex parte* review of whether a particular provider-defendant provided any

requested assistance and is entitled to statutory protection without the disclosure of sensitive national security information and resulting harm to national security. In this manner, the Act provides some basis for judicial review under special procedures, while avoiding the need to consider dismissal of these actions pursuant to the state secrets privilege. Dismissal under the FISA Act of 2008 should—and obviously would—moot the need to consider the Government's privilege assertion as a separate basis for dismissal.

The Attorney General's determination that the classified information in his certification, including the basis for his certification as to particular defendants, cannot be disclosed without causing exceptional harm to national security, is amply well-founded but cannot be described further on this record. *See* Classified Certification of the Attorney General of the United States.[9/]

CONCLUSION

For the foregoing reasons, all claims against the electronic communication service providers in this proceeding should be promptly dismissed.

September 19, 2008

Respectfully Submitted,

GREGORY G. KATSAS
Assistant Attorney General

CARL J. NICHOLS
Principal Deputy Associate Attorney General

JOHN C. O'QUINN
Deputy Assistant Attorney General

DOUGLAS N. LETTER
Terrorism Litigation Counsel

JOSEPH H. HUNT
Director, Federal Programs Branch

s/ Anthony J. Coppolino
ANTHONY J. COPPOLINO
Special Litigation Counsel

[9] To the extent the procedures in Section 802 do not result in dismissal of this action, then, as noted above, the state secrets privilege is not waived by the Act, *see* 50 U.S.C. § 1885a(h), and the United States does not waive or withdraw its prior state secrets and statutory privilege assertions in *Hepting* and *Verizon* actions, and for the reasons previously set forth in those assertions, dismissal of all the pending actions would continue to be required.

s/ Alexander K. Haas
ALEXANDER K. HAAS

s/ Paul G. Freeborne
PAUL G. FREEBORNE

Trial Attorneys
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW, Rm. 6102
Washington, D.C. 20001
Phone: (202) 514-4782—Fax: (202) 616-8460
Email: tony.coppolino@usdoj.gov

Attorneys for the United States