CINDY COHN (SBN 145997)
cindy@eff.org
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
MARK RUMOLD (SBN 279060)
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Fax: (415) 436-9993

RICHARD R. WIEBE (SBN 121156)
wiebe@pacbell.net
LAW OFFICE OF RICHARD R. WIEBE
One California Street, Suite 900
San Francisco, CA 94111
Telephone: (415) 433-3200
Fax: (415) 433-6382

RACHAEL E. MENY (SBN 178514)
rmeny@kvn.com
PAULA L. BLIZZARD (SBN 207920)
MICHAEL S. KWUN (SBN 198945)
AUDREY WALTON-HADLOCK (SBN 250574)
BENJAMIN W. BERKOWITZ (SBN 244441)
KEKER & VAN NEST, LLP
633 Battery Street
San Francisco, CA 94111
Telephone: (415) 391-5400
Fax: (415) 397-7188

THOMAS E. MOORE III (SBN 115107)
tmoore@moorelawteam.com
THE MOORE LAW GROUP
228 Hamilton Avenue, 3rd Floor
Palo Alto, CA 94301
Telephone: (650) 798-5352
Fax: (650) 798-5001

ARAM ANTARAMIAN (SBN 239070)
aram@eff.org
LAW OFFICE OF ARAM ANTARAMIAN
1714 Blake Street
Berkeley, CA 94703
Telephone: (510) 289-1626

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, TASH HEPTING, GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, *et al*.,

Defendants.

CASE NO. 08-CV-4373-JSW

PLAINTIFFS' FEDERAL RULE OF EVIDENCE SECTION 1006 SUMMARY OF VOLUMINOUS EVIDENCE FILED IN SUPPORT OF THEIR MOTION FOR PARTIAL SUMMARY JUDGMENT AND OPPOSITION TO THE GOVERNMENT DEFENDANTS' CROSS-MOTION

Date: December 14, 2012
Time: 9:00 a.m.
Courtroom 11, 19th Floor
The Honorable Jeffrey S. White

TABLE OF CONTENTS

I. INTRODUCTION

Plaintiffs respectfully submit the following Summary of Voluminous Evidence pursuant to Fed. R. Evid. 1006, compiling into one document with a supporting declaration and exhibits a broad swath of currently available public evidence supporting plaintiffs' claims.

Rule 1006 does not require that "'it be literally impossible to examine the underlying records.'" *U.S. v. Stephens*, 779 F.2d 232, 238-39 (5th Cir. 1985) (quoting *U.S. v. Scales*, 594 F.2d 558, 562 (6th Cir. 1978), cert. denied, 441 U.S. 946 (1979)). "The fact that the underlying documents are already in evidence does not mean that they can be 'conveniently examined in court.'" *Stephens*, 779 F.2d at 239 (quoting *U.S. v. Lemire*, 720 F.2d 1327, 1347 (D.C. Cir. 1983)).

Plaintiffs submit this Summary of Voluminous Evidence in support of their Fed. R. Civ. Pro. 56(d) declaration, in that the Summary reflects the substantial breadth of information in the public domain that would be subject to discovery, particularly from government sources. Plaintiffs also submit this Summary in opposition to the government's contention that plaintiffs cannot prove their case, especially injury in fact, due to the state secrets privilege. Plaintiffs further submit this Summary to highlight the governments' use of certain key terms including "surveillance," "content," and "collect" in a way that tends to create a misleading impression.

Fed. R. Evid. 1006 is the appropriate vehicle for putting the evidence before the Court. The writings that plaintiffs are summarizing are voluminous, and the plaintiffs have produced those writings to the government and to the Court. Rule 1006 requires that the summary document be based on foundation testimony connecting it with underlying evidence summarized, and must fairly represent competent evidence already before the trier of fact. *Fagiola v. Nat'l Gypsum Co. AC & S., Inc.,* 906 F.2d 53, 57 (2d Cir. 1990) ("Evidence admitted under Rule 1006 must be otherwise admissible and remains subject to the usual objections under the rules of evidence and the Constitution."); *see also U.S. v. Milkiewicz*, 470 F.3d 390, 396 (1st Cir. 2006).

However, at the summary judgment stage, the non-moving party need not produce evidence in a form that is admissible at trial in order to avoid summary judgment. *Celotex Corp. v. Catrett*, 477 U.S. 317, 324 (1986). Thus, in examining the evidence of a party opposing summary

judgment, courts do not focus on the admissibility of the evidence's form, but rather on the potential admissibility at trial of its contents. *Fraser v. Goodale*, 342 F.3d 1032, 1036-37 (9th Cir. 2003) (citing *Block v. City of Los Angeles*, 253 F.3d 410, 418-19 (9th Cir. 2001) ("To survive summary judgment, a party does not necessarily have to produce evidence in a form that would be admissible at trial, as long as the party satisfies the requirements of Federal Rules of Civil Procedure 56."). For example, even if a statement quoted in a book or a newspaper article is hearsay, the information asserted in such an article would be admissible in a subsequent trial through the testimony of the person quoted, or by establishing the foundation for a hearsay exception or showing that the statement was a non-hearsay admission.

Moreover, at this stage in the litigation, the Court is entitled to use circumstantial evidence and to draw inferences therefrom. *In re Sealed Case*, 494 F.3d 139, 147 (D.C. Cir. 2007). Accordingly, for purposes of this motion, the Court may consider all of the evidence contained in this Summary of Evidence. Moreover, many of the writings are admissible as admissions of an opposing party (Fed. R. Evid. 801(c)(2)) or as a public record (Fed. R. Evid. 902). To the extent that a writing might be inadmissible, plaintiffs submit the writing to show that an opportunity to conduct discovery will likely yield admissible evidence that would support plaintiffs' opposition to the government's motion.

II. THE PRESIDENT'S SURVEILLANCE PROGRAM

A. Overview of the Program

Shortly after the September 11, 2001 terrorist attacks, President George W. Bush authorized the National Security Agency to conduct a variety of surveillance activities, including the warrantless surveillance of telephone and Internet communications of persons within the United States. Department of Defense, *et al*., Offices of Inspector Gen., *Unclassified Report on the President's Surveillance Program* (July 10, 2009) at 1 ("OIG PSP Report")[1] [Vol. III, Ex. 33, p.

[1] Unless otherwise noted, all citations to evidence summarized herein are to evidence introduced through the Declaration of Kurt Opsahl Regarding Plaintiffs' Evidence and Rule 1006 Summary of Voluminous Evidence Filed in Support of Plaintiffs' Motion for Partial Summary Judgment and Opposition to the Government Defendant's Cross Motion ("Opsahl Declaration"). For clarity, each citation to plaintiffs' voluminous evidence, filed herewith, will provide a description of the

1197][2] Declaration of Lt. Gen. Keith B. Alexander (MDL Dkt. No. 06-cv-01791) (Dkt. # 254-4) at ¶ 10 [Vol. IV, Ex. 77, p. 2539].[3] The OIG PSP Report termed these surveillance activities the "President's Surveillance Program" (hereafter, "the Program"). OIG PSP Report at 1 [Vol. III, Ex 33, p. 1197]. The Program is broader than the narrow subset of surveillance activities that, in 2005, the Bush Administration decided to label the "Terrorist Surveillance Program" (hereafter, "TSP"). *Id*. at 1-2, 5-6, 36-37 [pp. 1197-98, 1201-02, 1232-33].

A secret presidential order (the "Program Order"), signed on October 4, 2001, expanded the authority of the NSA "to conduct electronic surveillance within the United States without an order from the [Foreign Intelligence Surveillance Court (FISC)]." OIG PSP Report at 5 [Vol. III, Ex. 33, p. 1201].[4] The Program began on October 6, 2001, prior to any comprehensive legal review by the Department of Justice. *Id.* at 11 [p. 1207]; *Nomination of Gen. Michael Hayden to be the Dir. of the Central Intelligence Agency*, Hearing of the S. Select Comm. on Intelligence, 109th Cong. at 62 (May 18, 2006) ("Hayden Hearing") [Vol. I, Ex. 2, p. 65]. The Program Order permitted the NSA to carry out a variety of new intelligence activities within the United States. OIG PSP Report at 5-6 [Vol. III, Ex. 33, pp. 1201-02]. President Bush renewed the Program Order at least 30 times, approximately every 45 days. *Id*. at 1, 7 [pp. 1197, 1203]; Letter from Shannen W. Coffin, Counsel to the Vice President, Office of the Vice President, to Sen. Patrick J. Leahy, Chairman, S. Comm.

---

document being cited, followed by its location in the record by volume, exhibit, and control number.

[2] "Title III of the Foreign Intelligence Surveillance Act Amendments Act (FAA) of 2008 required the Inspectors General of the elements of the intelligence community that participated in the President's Surveillance Program to conduct a comprehensive review of the program. The IGs of the Department of Justice, the Department of Defense, the Central Intelligence Agency, the National Security Agency, and the Office of the Director of National Intelligence participated in the review required by the Act." OIG PSP Report. [p. 1194]

[3] *See also* James Risen & Eric Lichtblau, *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. TIMES (Dec. 24, 2005) [Vol. IV, Ex. 66, pp. 1714 - 16]; James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005) [Vol. IV, Ex. 72, pp. 1764 – 69]; Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY (May 11, 2006) [Vol. III, Ex. 30, pp. 1182-85].

[4] *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005) [Vol. IV, Ex. 72, p. 1764-69]; ERIC LICHTBLAU, BUSH'S LAW: THE REMAKING OF AMERICAN JUSTICE 157 (Pantheon Books 2008) ("BUSH'S LAW") [Vol. I, Ex. 1, p. 3.022].

on the Judiciary, and Sen. Arlen Specter, Ranking Minority Member, S. Comm. on the Judiciary (Aug. 20, 2007) ("OVP Subpoena Response") [Vol. I, Ex. 3, pp. 175-77].[5]

The entire Program remained secret until newspaper reports – a series of December 2005 *New York Times* articles, a December 2005 *Los Angeles Times* article, and a May 2006 *USA Today* article – revealed two discrete aspects of the Program: the warrantless surveillance of Internet and telephone communications and the government's acquisition of domestic call-detail records from major telecommunications carriers. OIG PSP Report at 6 [Vol. III, Ex. 33, p. 1202]; Barton Gellman & Arshad Mohammed, *Data on Phone Calls Monitored; Extent of Administration's Domestic Surveillance Decried in Both Parties*, WASH. POST (May 12, 2006) [Vol. III, Ex. 35, p. 1255]. While the precise scope of the surveillance activities and the legal arguments used to support the Program have fluctuated over time, OIG PSP Report at 1 [p. 1197], to date, the Program remains in operation, largely unchanged from its original form. *See* Section III(D)-(E), *infra* at 42-44.

B. Evidence Showing How the Program Operates

Plaintiffs' evidence and statements by government officials demonstrate that the Program has at least two components: the acquisition, analysis, and storage of international and domestic communications, and the acquisition and analysis of historical call-detail records obtained from telecommunications carriers.

The first disclosure of the Program's operation came in a series of articles in December 2005, in which the *New York Times* publicly disclosed for the first time that "President Bush

[5] In response to a June 27, 2007 subpoena issued by the Committee on the Judiciary to the Office of the Vice President relating to past warrantless electronic surveillance, the Office of the Vice President identified 43 Program Orders (and two amended Program Orders) (identified as Top Secret/Codeword Presidential Authorizations) between October 4, 2001 and December 2006. OVP Subpoena Response [Vol. I, Ex. 3, pp. 175 - 77]. The identified dates were October 4, November 2, and November 30, 2001; January 9, March 14, April 18, May 21, June 24, July 30, September 10, October 15, and November 18, 2002; January 8, February 7, March 17, April 22, June 11, July 14, September 10, October 15 and December 9, 2003; January 14, March 11 (including as amended by the Presidential Memoranda of March 19 and April 2), May 5, June 23, August 9, September 17, and November 17, 2004; January 11, March 1, April 19, June 14, July 26, September 10, October 26, and December 13, 2005; and January 27, March 21, May 16, July 6, September 6, October 24, and December 8, 2006. *Id*.

secretly authorized the National Security Agency to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required for domestic spying." James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005) [Vol. IV, Ex. 72, pp. 1764-69]; James Risen & Eric Lichtblau, *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. TIMES (Dec. 24, 2005) [Vol. IV, Ex. 66, pp. 1714-16]. The articles further disclosed that, "by tapping directly into some of the American telecommunications system's main arteries," the NSA had "traced and analyzed large volumes of telephone and Internet communications flowing into and out of the United States as part of the eavesdropping program." Risen & Lichtblau, *Spy Agency Mined Vast Data Trove* at 1 [Vol. IV, Ex. 66, p. 1714]. But the media statements are not the only evidence. Statements by multiple government officials confirm the aspect of the Program reported by the *Times*. The eyewitness and directed documentary evidence presented by plaintiffs in this Summary of Voluminous Evidence, further confirms those government admissions and media reports.

In May 2006, an article in *USA Today* publicly disclosed a separate aspect of the Program: the secret collection of "phone call records of tens of millions of Americans, using data provided by" the nation's largest telecommunications carriers. Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY (May 11, 2006) [Vol. III, Ex. 30, p. 1182].[6] The NSA then uses the call-records data to examine how "networks contact each other and how they are tied together." *Id.* [p. 1183]. And, like the aspect of the Program disclosed by the *Times*, the call records program was "conducted without warrants and without the approval of the FISA court." *Id*. [p. 1184]. As described in detail below, numerous statements by government officials confirm the media reports.

[6] In fact, some of the activities reported in the *USA Today* article had previously been reported by the *Los Angeles Times*. Joseph Menn & Josh Meyer, *U.S. Spying is Much Wider, Some Suspect*, L.A. TIMES (Dec. 25, 2005) [Vol. III, Ex. 36, p. 1258]. However, the report published by *USA Today* spurred multiple congressional inquiries and official government confirmations on this portion of the Program. *See Section* II(B)(2)*, infra* at 19-24.

1. Evidence of Communications Surveillance

(a) Wholesale Acquisition of International and Domestic Telephone and Internet Communications

The government conducts communications surveillance under the Program in several stages, starting with acquisition of the communications passing through major telecommunications switches. Government officials confirmed to the *New York Times* that the NSA obtained "backdoor access to streams of domestic and international communications" via arrangements with "some of the nation's largest telecommunications companies." Risen & Lichtblau, *Spy Agency Mined Vast Data Trove* at 1-2 [Vol IV, Ex. 66, pp. 1714-15].[7] Those agreements provided the NSA "access to major telecommunications switches on American soil." *Id*. at 3 [p. 1716].

Plaintiffs' eyewitness evidence confirms that Program surveillance begins with wholesale acquisition of communications – both international and domestic – from domestic telecommunications switches. In January 2006, a former AT&T employee named Mark Klein[8] provided detailed eyewitness testimony and documentary evidence showing how the government, in partnership with AT&T, acquires access to the streams of international and domestic communications. Declaration of Mark Klein ("Klein Decl.") ¶¶ 10-36 (unredacted version filed under seal at Dkt. #84-1) [Vol. VII, Ex. 115, pp 4716-22].[9]

---

[7] *See also* Shane Harris & Tim Naftali, *Tinker, Tailor, Miner, Spy: Why the NSA's Snooping Is Unprecedented In Scale and Scope*, SLATE (Jan. 3, 2006) [Vol. IV, Ex. 67, pp. 1718-19] (As part of the Program, "[telecommunications] companies have granted the NSA access to their all-important switches, the hubs through which colossal volumes of voice calls and data transmissions move every second…. [T]he NSA appears to be vacuuming up all data, generally without a particular phone line, name, or e-mail address as a target.").

[8] Klein is a former AT&T Corp. employee who retired in May 2004. Klein Decl. ¶¶ 2-6 [Vol. VII, Ex. 115, p. 4717]. In the period relevant to this motion, he worked at a facility that handled AT&T's WorldNet International Service ("Geary Facility"), *id.* ¶¶ 8-9 [pp. 4717-18], and at the Folsom Street Facility which handled AT&T's WorldNet International Service, such as dial-up and DSL Internet service. *Id.* ¶¶ 15, 19 [pp. 4718, 4719].

[9] *See also* JAMES RISEN, STATE OF WAR: THE SECRET HISTORY OF THE CIA AND THE BUSH ADMINISTRATION 48 (Simon & Schuster 2006) ("STATE OF WAR") [Vol. III, Ex. 60, p. 1609.013] ("NSA's technical prowess, coupled with its long-standing relationships with the nation's major telecommunications companies, has made it easy for the agency to eavesdrop on large numbers of people in the United States without their knowledge. Following President Bush's order, U.S. intelligence officials secretly arranged with top officials of major telecommunications companies to gain access to large telecommunications switches carrying the bulk of America's phone calls.

Klein's job at AT&T was "to oversee the WorldNet Internet room" at AT&T's Folsom Street facility in San Francisco. *Id.* ¶ 15 [p. 4718]. Communications carried by AT&T's WorldNet Internet service pass through that room to be directed to or from customers of AT&T and other service providers. *Id.* ¶ 19 [p. 4719]. The WorldNet Internet Room is designed to process vast amounts of electronic communications traffic "peered"[10] by AT&T between its Common Backbone ("CBB")[11] Internet network and other carriers' networks. *Id*. ¶ 22 [p. 4720]. The Folsom Street Facility also handles millions of telephone communications. *See id.* ¶ 13 [p. 4718].

The Klein evidence describes how the government initially intercepts Internet communications, which are carried as light signals on fiber-optic cables. *Id.* ¶¶ 21-24 [p. 4720]; *see also* Declaration of J. Scott Marcus ¶ 52 [Vol. VII, Ex. 116, p. 4756]. To divert the stream of communications to the government, AT&T connected the fiber-optic cables entering its WorldNet Internet room to a "splitter cabinet." Klein Decl. ¶¶ 19, 25-34 [Vol. VII, Ex. 115, pp. 4719, 4720-21].

The "splitter cabinet" splits the light signals from the WorldNet Internet service in two, making two identical copies of the data carried on the light signal. *Id.* ¶ 24 [p. 4720]. The splitter cabinet directs one copy of the light signal through fiber optic cables into a secret room built on AT&T premises, but controlled by the NSA, while allowing the other copy to travel its normal course to its intended destination. *Id.* ¶¶ 27-34 [pp. 4720-21]. The split cables carry both domestic and international communications of AT&T customers, as well as communications from users of other non-AT&T networks that pass through the Folsom Street Facility. *Id.* ¶¶ 31-34 [p. 4721]. The

---

The NSA also gained access to the vast majority of American e-mail traffic that flows through the U.S. telecommunications system.")

[10] "Peering" is the process whereby Internet providers interchange traffic destined for their respective customers, and for customers of their customers. *See* Marcus Decl. ¶¶ 96-98 [Vol. VII, Ex. 116, p. 4767-68].

[11] AT&T's Common Backbone network, like backbone networks generally, is used for the transmission of interstate or foreign communications. An Internet backbone can be thought of as a large Internet Service Provider (ISP), many of whose customers may themselves be smaller ISPs. There is no single network that is *the Internet*; rather, the Internet backbones collectively form the core of the global Internet. *See* Marcus Decl. nn. 5-6, at 3 [Vol. VII, Ex. 116, p. 4748].

use of the splitter cabinet to create an identical copy results in the wholesale acquisition by the government of AT&T customers' Internet communications. *Id*. ¶¶ 22-36 [pp. 4720-22].[12]

Plaintiffs retained an expert in information technology and telecommunications to explain the implications of the documents and testimony Klein furnished. *See generally* Declaration of J. Scott Marcus ("Marcus Decl.") [Vol. VII, Ex. 116, pp. 4743-5070]. The expert, J. Scott Marcus, spent decades working for a variety of telecommunications clients, including AT&T, and served as a senior technical advisor for Internet technology to the Federal Communications Commission ("FCC") from July 2001 until July 2005 and as a member of the FCC's Homeland Security Policy Council. *Id*. ¶¶ 7-29 [pp. 4747-4751].

In particular, Marcus explains that the location of the fiber split in AT&T's network was not designed to capture only international traffic, but to intercept purely domestic communications as well. *Id.* ¶¶ 107-11 [pp. 4770-71]. A substantial amount of AT&T's peered traffic in San Francisco was acquired by the surveillance configuration described by Klein, including nearly all of the peered international communications carried at the Folsom Street Facility, and a substantial amount of domestic Internet traffic. *Id.* ¶¶ 47-49; 91-111 [pp. 4755-56, 4767-4771].

While Klein's evidence establishes AT&T's participation in the Program at its San Francisco location, from the arrangement of the hardware, plaintiffs' expert Marcus concluded that AT&T's surveillance "apparently involves considerably more locations than would be required to catch the majority of international traffic." Marcus Decl. ¶ 43 [p. 4755]. Further evidence confirms the expert's view. Klein reports "that other such 'splitter cabinets' were being installed in other cities, including Seattle, San Jose, Los Angeles and San Diego." Klein Decl. ¶ 36 [Vol. VII, Ex.

[12] *See also* Siobhan Gorman, *NSA's Domestic Spying Grows As Agency Sweeps Up Data*, WALL ST. J. (Mar. 10, 2008) at 4 [Vol. IV, Ex. 95, p. 3026] ("Current and former intelligence officials say . . . [telecommunication companies] are giving the government unlimited access to a copy of the flow of communications, through a network of switches at U.S. telecommunications hubs that duplicate all the data running through it."); Seymour Hersh, *Listening In*, NEW YORKER (May 29, 2006) [Vol. IV, Ex. 79, p. 2711] (Seymour Hersh reporting that "[a] security consultant working with a major telecommunications carrier told me that his client set up a top-secret high-speed circuit between its main computer complex and . . . the site of a government-intelligence computer center," providing "total access to all the data").

115, p. 4722].[13] According to Marcus, a web of similar surveillance facilities would probably capture well over half of AT&T's purely domestic traffic, representing almost all of the AT&T traffic to and from other providers. Marcus Decl. ¶¶ 122-127 [Vol. VII, Ex. 116, pp. 4774-75]. Thus, the government would have access to "*10% of all purely domestic Internet communications in the United States*," including non-AT&T customers. *Id.* at ¶¶ 5, 125 [pp. 4746, 4775] (emphasis in original) (evidence indicates AT&T Corp. has "given the government direct access to telecommunications facilities physically located on U.S. soil; that, by virtue of this access, the government would have the capacity to monitor both domestic and international communications of person in the United States").[14]

In addition to plaintiffs' eyewitness evidence, government officials with knowledge of the Program have confirmed media reports on the Program on multiple occasions. Consistent with the installation of surveillance capabilities on the peered networks of AT&T facilities, the communications targeted by the NSA, as Gen. Michael Hayden[15] noted, "coexisted out there in a great global web with your phone calls and my e-mails." Remarks by Gen. Michael Hayden, *Address to the National Press Club*, Washington, D.C. (Jan. 23, 2006) [Vol. IV, Ex. 73, p. 1800]. This requires the NSA, as noted by Rep. Peter Hoekstra,[16] "to steal light off of different cables" in

---

[13] *See also* Kim Zetter, *Is the NSA spying on U.S. Internet traffic?*, SALON MAGAZINE (June 21, 2006) [Vol. IV, Ex. 75, p. 2453] (reporting that, at AT&T's Bridgton technical command center in St. Louis, "AT&T has maintained a secret, highly secured room since 2002 where government work is being conducted" and that "only government officials or AT&T employees with top-secret security clearance are admitted to the room").

[14] *See also* Gorman, *NSA's Domestic Spying Grows As Agency Sweeps Up Data* [Vol. IV, Ex. 95, p. 3028] ("Current and former intelligence officials confirmed a domestic network of hubs, but didn't know the number.").

[15] Gen. Hayden was the Director of the NSA from March 1999 - April 2005, Principal Deputy Director of National Intelligence from April 2005 - May 2006, and Director of the CIA from 2006 - February 2009. *See* Biographies, Michael Hayden, U.S. Air Force, *available at* http://www.af.mil/information/bios/bio.asp?bioID=5746.

[16] Rep. Hoekstra was "read in" to the Program on September 23, 2004. Letter from John D. Negroponte, Dir. of Nat'l Intelligence, to J. Dennis Hastert, Speaker of the U.S. House of Representatives (May 17, 2006), at 2-3 [Vol. IV, Ex. 85, p. 2770] (listing briefings that Rep. Hoekstra received about the Program). "The process of being 'read in' to a compartmented program generally entails receiving a briefing about the program followed by a formal acknowledgement of the briefing, usually indicated by the signing of a Nondisclosure Agreement binding the individual to obligations regarding the handling and use of information concerning the

order to acquire the "information that's most important to us." Interview with Rep. Peter Hoekstra by Paul Gigot, *Lack of Intelligence: Congress Dawdles on Terrorist Wiretapping,* JOURNAL EDITORIAL REPORT, FOX NEWS CHANNEL (Aug. 6, 2007) at 2 [Vol. II, Ex. 14, p. 714]; *see also* OIG PSP Report at 15 [Vol. III, Ex. 33, p. 1211].

According to former Senator Bob Graham, who chaired the Intelligence Committee at the time, briefers told him that "Bush had authorized . . . the NSA to intercept 'conversations that . . . went through a transit facility inside the United States.'" Barton Gellman, *et al*., *Surveillance Net Yields Few Suspects*, WASH. POST at 3 (Feb. 5, 2006) [Vol. IV, Ex. 68, p. 1748]; *see also* Lichtblau & Risen, *Spy Agency Mined Vast Data Trove* at 1 [Vol. IV, Ex. 66, p. 1714] (quoting a government official stating, "There was a lot of discussion about the switches. . . . You're talking about access to such a vast amount of communications, and the question was, How do you minimize something that's on a switch carrying such large volumes of traffic?").

Finally, as the surveillance configuration described by the Klein evidence shows, the Program acquires vast amounts of innocent Americans' communications. Klein Decl. ¶¶ 24-36 [Vol. VII, Ex. 115, pp. 4720-22]; Marcus Decl. ¶¶ 122-27 [Vol. VII, Ex. 116, pp. 4774-75]. In an interview with PBS's Frontline, James Baker, former head of the Justice Department's Office of Intelligence Policy and Review (who is read in to the Program),[17] agreed that the following description was a "fair assessment" of the Program's operation:

> So what you're saying is that with modern communications, it's almost inevitable that you're going to collect, *in the sense of initially acquire*, communications of innocent people, of Americans who are not suspected of terrorism[.]

PBS Frontline, *Spying on the Homefront*, Interview with James A. Baker at 7 (March 2, 2007) [Vol. II, Ex. 23, p. 1053]; *see also* PBS Frontline, *Spying on the Homefront*, Interview with John C.

---

program." Dept. of Justice, Office of the Inspector Gen., *Report of Investigation Regarding Allegations of Mishandling of Classified Documents by Att'y Gen. Alberto Gonzales* (Sept. 2, 2008) ("OIG Gonzales Report") at 8, n.10 [Vol. I, Ex. 7, p. 363].

[17] *See The Foreign Intelligence Surveillance Act*: *Hearing before the H. Permanent Select Comm. on Intelligence*, 110th Cong. at 86 (Sept. 18, 2007) (James Baker was briefed on the Program in late 2001) [Vol. I, Ex. 5, p. 307].

Yoo at 3 (Jan. 10, 2007) [Vol. I, Ex. 10, p. 393] (noting that the government "needs to have at least access to the flow [of communications];. . . In order to get Internet messages, you have to be able to dip into the flow of communications, because Internet communications are broken up. . . . I don't think it's inherently always wrong for communications providers to give the government access to the networks.")

Thus, both plaintiffs' evidence and statements by government officials confirm the *New York Times* reporting that the initial stages of the Program involve the wholesale acquisition of communications from the streams of domestic telecommunications network.

(b) Automated Analysis, or Datamining, of Content and Non-Content Information

Once the communications are acquired, the Program involves "comb[ing] through large volumes of phone and internet traffic" in a "large data-mining operation." Lichtblau & Risen, *Spy Agency Mined Vast Data Trove* at 1 [Vol. IV, Ex. 66, p. 1714].

The facts underlying this reporting have been admitted to by the government. As former Homeland Security Secretary Michael B. Chertoff confirmed in a January 2006 interview, the Program involves "'data-mining' – collecting vast amounts of international communications data, running it through computers to spot key words and honing in on potential terrorists." Morton Kondracke, *NSA Data Mining is Legal, Necessary, Chertoff Says,* ROLL CALL at 1 (Jan. 19, 2006) [Vol. IV, Ex. 69, p. 1753] ("[W]hat we're trying to do is gather as many dots as we can, figure out which are the ones that have to be connected and we're getting them connected" by "sift[ing] through an enormous amount of data very quickly[.]);[18] Letter from Kathleen Turner, Dir. of Leg. Affairs, Office of the Dir. of Nat'l Intelligence, to Rep. Silvestre Reyes, Chairman, and Rep. Peter Hoekstra, Ranking Member of the H. Intelligence Comm. ("Turner Letter"), at p. 5, 6 of

[18] *See also* Harris & Naftali, *Why the NSA's Snooping Is Unprecedented In Scale and Scope* at 1 [Vol. IV, Ex.67, p. 1718] (As early as 2001, "the NSA approached U.S. carriers and asked for their cooperation in a 'data-mining' operation, which might eventually cull 'millions' of individual calls and e-mails.").

attachment [Vol. II, Ex. 22, pp. 1042, 1043] (noting "Intelligence analysts must comb through extremely large amounts of data to do their job").[19]

According to John Yoo, a former Department of Justice official assigned to oversee the Program, NSA surveillance activities should be geared toward "look[ing] at all email, text and phone traffic between Afghanistan and Pakistan and the U.S," which "involve[s] the filtering of innocent traffic, just as roadblocks and airport screenings do." John Yoo, Op-Ed., *Why We Endorsed Warrantless Wiretaps*, WALL ST. J. at 2 (July 16, 2009) [Vol. V, Ex. 107, p. 4013]. To facilitate this filtering, Yoo explained, "you need to have computers to do it, where we have computers that are able to search through communications and are able to pluck out e-mails [and] phone calls that have a high likelihood of being terrorists' communications." PBS Frontline, *Spying on the Homefront*, Interview with John C. Yoo at 5 (Jan. 10, 2007) [Vol. I, Ex. 10, p. 395]; *see also* Gellman, *Surveillance Net Yields Few Suspects* at 4 [Vol. IV, Ex. 68, p. 1749] (quoting Senator Arlen Spector referring to "'mechanical surveillance' that is taking place before U.S. citizens and residents are 'subject to human surveillance'").[20]

These descriptions of the Program are consistent with plaintiff's evidence, as described further below. The AT&T documents presented by Mr. Klein show that a Narus STA 6400 was

---

[19] *See also* Gorman, *NSA's Domestic Spying Grows As Agency Sweeps Up Data* at 2 [Vol. IV, Ex. 95, p. 3024] ("Two former officials familiar with the data-sifting efforts said they work by starting with some sort of lead, like a phone number or Internet address. . . .[T]he systems then can track all domestic and foreign transactions of people associated with that item -- and then the people who associated with them, and so on, casting a gradually wider net. An intelligence official described more of a rapid-response effect: If a person suspected of terrorist connections is believed to be in a U.S. city . . . the government's spy systems may be directed to collect and analyze all electronic communications into and out of the city.").

[20] *See also* Gellman, *Surveillance Net Yields Few Suspects* at 1, 5 [Vol. IV, Ex. 68, pp. 1746, 1750] ("Surveillance takes place in several stages, officials said, the earliest by machine. Computer-controlled systems collect and sift basic information about hundreds of thousands of faxes, emails and telephone calls into and out of the United States before selecting the ones for scrutiny by human eyes an ears... [T]his kind of filtering intrudes into content, and machines 'listen' to more Americans than humans do."); STATE OF WAR 48 [Vol. III, Ex. 60, p. 1609.013] (The Program "employ[s] extremely powerful computerized search programs—originally intended to scan foreign communications—in order to scrutinize large volumes of American communications."); Seymour Hersh, *Listening In* at 2 [Vol. IV, Ex. 79, p. 2712] ("[T]he N.S.A. began, in some cases, to eavesdrop on callers (often using computers to listen for key words) …").

installed in NSA's secure room inside of AT&T's Folsom Street facility. Klein Decl. at ¶ 35 [Vol. VII, Ex. 115, pp. 4721-22]. As plaintiffs' expert J. Scott Marcus explains, the Narus machine is a "semantic traffic analyzer" – a device "designed to capture data directly from a network, apply a structured series of tests against the data, and respond appropriately." Marcus Decl. ¶¶ 79, 80 [Vol. VII, Ex. 116, p. 4763]. The Narus machine has the capability "to process huge volumes of data, including user content, in real time." *Id*. ¶ 83 [p. 4764]. Thus, the configuration deployed in the secure room is "well suited to the capture and analysis of large volumes of data for surveillance purposes." *See id*. [p. 4764]; Declaration of William E. Binney ("Binney Decl.") ¶¶ 8, 10 [Vol. VII, Ex. 118, pp. 5074, 5075] (Narus device would select for predetermined data including "target addresses, locations, countries, and phone numbers, as well as watch-listed names, keywords, and phrases."); *see also* Gellman, *Surveillance Net Yields Few Suspects* at 4 [Vol. IV, Ex. 68, p. 1749] (according to former NSA Inspector General Joel F. Brenner, the agency has "no choice but to rely on 'electronic filtering, sorting and dissemination systems of amazing sophistication but that are imperfect.'").[21]

Thus, statements by government officials, media reports and plaintiffs' evidence all demonstrate that the Program operates by mining communications data after the communications' initial wholesale acquisition.

---

[21] Indeed, the efficacy of data mining as a tool to fight terrorism has been sharply questioned. A 352-page study by the National Research Council (part of the congressionally-chartered National Academy of Sciences) reports that data mining is not an effective tool in the fight against terrorism. *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention*, National Research Council, Executive Summary at 3-4 (2008) [Vol. II, Ex. 18 pp. 911-2].

Those findings are confirmed by the experience of American intelligence agents' use of Program-generated information. According to one FBI official familiar with the Bureau's use of NSA data, agents would "chase a number, find it's a school teacher with no indication they've ever been involved in international terrorism - case closed. . . . After you get a thousand numbers and not one is turning up anything, you get some frustration." Lowell Berman, *et al.*, *Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends*, N.Y. TIMES (Jan. 17, 2006) [Vol. IV, Ex. 80, p. 2715]. Within the FBI, "the N.S.A. material continued to be viewed as unproductive, prompting agents to joke that a new bunch of tips meant more 'calls to Pizza Hut,' one official, who supervised field agents, said." *Id*. at 3 [p. 2717].

According to Jeff Jonas, now chief scientist at IBM Entity Analytics, pattern matching techniques that "'look at people's behavior to predict terrorist intent . . . are so far from reaching the level of accuracy that's necessary that I see them as nothing but civil liberty infringement engines.'" Gellman, *Surveillance Net Yields Few Suspects* at 5 [Vol. IV, Ex. 68, p. 1750].

(c) Communications are not Minimized Prior to Storage

Prior to human review, the acquired communications — including those to, from, and/or between Americans, as well as those communications without any foreign intelligence value — are stored in a vast government database.

The process through which the intelligence community has traditionally reduced the privacy intrusion caused by electronic surveillance is known as "minimization" — "procedures for reviewing, handling, and, as appropriate, destroying, information about U.S. persons, depending on whether or not the information constitutes foreign intelligence information." Letter from Alexander Joel, Office of the Dir. of Nat'l Intelligence, to Rep. Silvestre Reyes and Rep. Peter Hoekstra (Sept. 17, 2007) [Vol. I, Ex. 5, p. 313]. According to former Director of National Intelligence ("DNI") J. Michael McConnell, "[t]he minimization procedures that Intelligence Community agencies follow are Attorney General approved guidelines issued pursuant to Executive Order 12333. These minimization procedures apply to the acquisition, retention and dissemination of U.S. person information." *The Foreign Intelligence Surveillance Act and Implementation of the Protect America Act*: Hearing before the S. Comm. on the Judiciary, 110th Cong. (Sept. 25, 2007) (Statement of J. Michael McConnell, Dir. of Nat'l Intelligence) at 13 [Vol. II, Ex. 20, p. 1023].

However, as McConnell explained, under Program surveillance, immediately after acquisition "there is no human that is aware of it. So you wouldn't know that [communications without foreign intelligence value were there] until you went into the database." *Foreign Intelligence Surveillance Act:* Hearing before the Permanent H. Select Comm. on Intelligence, 110th Cong. at 91 (Sept. 20, 2007) (testimony of J. Michael McConnell, Dir. of Nat'l Intelligence) ("Sept. 20, 2007 McConnell Testimony") [Vol. IV, Ex. 98, p. 3220].

McConnell further admitted that the communications are acquired and placed in a database *before* minimization. In response to a question on the number of Americans whose communications had been intercepted, he testified:

> MR. MCCONNELL: I am not even sure we keep information in that form. It would probably take us some time to get the answer. The reason is, you're collecting information. It is in a file. It will roll off in a period of time. You may not even

> know it is in the database. That is one of the reason we are so careful about who has access to that database. . . .
>
> REP. BERMAN: . . . How do you minimize without knowing?
>
> MR. MCCONNELL: If you look at it, then you know.
>
> REP. BERMAN: So all you do is minimize the ones you happen to look at.
>
> MR. MCCONNELL: Right. If there is something in there that — it doesn't come up for some reason, you just wouldn't know. …

Warrantless Surveillance And The Foreign Intelligence Surveillance Act: The Role Of Checks And Balances In Protecting Americans' Privacy Rights (Part II): Hearing before the H. Comm. on the Judiciary, 110th Cong. at 79 (Sept. 18, 2007) [Vol. II, Ex. 17, p. 812] (testimony of J. Michael McConnell, Dir. of Nat'l Intelligence) ("Sept. 18, 2007 McConnell Testimony"); Sept. 20, 2007 McConnell Testimony at 91 [Vol. IV, Ex. 98, p. 3220] (only "once there is some reason to look at data" can the government track the number of U.S. persons involved).

Likewise, in testimony before the Senate Judiciary Committee, the following exchange took place:

> FEINSTEIN: . . . Do the minimization procedures prevent NSA from retaining communications that do not contain foreign intelligence information?
>
> MCCONNELL: If recognized, the minimization would require them to expunge it from the database. . . .
>
> FEINSTEIN: So what is the minimization process? And how does it function? And what happens with that collection?
>
> MCCONNELL: The – first of all, you may not even realize it's in the database, because you do lots of collection, you have to have a reason to look.

Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?: Hearing before the S. Comm. on the Judiciary, 110th Cong. at 23, 26 (Sept. 25, 2007) [Vol. II, Ex. 19, pp. 961, 964] (testimony of J. Michael McConnell, Dir. of Nat'l Intelligence); *see also* Sept. 20, 2007 McConnell Testimony at 91 [Vol. IV, Ex. 98, p. 3220] ("We may not know that is in the database until we have some reason to go query that portion of the database for foreign intelligence purpose.").

The inference from former DNI McConnell's statement is that communications between U.S. persons and records of such communications are in the database – and remain in the database – available for human intelligence analysts to review. Because there are "billions of things going on" in the database, McConnell explained, information without foreign intelligence value will remain stored for some period of time if it "hasn't been examined." Sept. 20, 2007 McConnell Testimony at 69 [Vol. IV, Ex. 98, p. 3198]. Indeed, former Attorney General Alberto Gonzales suggested in sworn testimony before Congress that, once collected, the information is kept indefinitely, even if the subject of the surveillance is an ordinary American: "In terms of what is actually done with that information, . . . information is collected, information is retained and information is disseminated . . . ." *Wartime Executive Power and the NSA's Surveillance Authority:* Hearing before the S. Comm. on the Judiciary, 109th Cong. 42 (Feb. 6, 2006) [Vol. V, Ex. 104, p. 3722] (testimony of Alberto Gonzalez) (included as an attachment to Plaintiffs' Request for Judicial Notice, *Hepting v. AT&T Corp*. 06-CV-00672 (Mar. 31, 2006) (Dkt. # 20-1)) ("March 2006 RJN").

As a result of the government's data collection, "[p]articipants, according to a national security lawyer who represents one of them privately, are growing 'uncomfortable with the mountain of data they have now begun to accumulate.'" Gellman, *Surveillance Net Yields Few Suspects* at 2 [Vol. IV, Ex. 68, p. 1747].

(d) Minimization Does not Adequately Protect the Privacy Interests of U.S. Persons Whose Domestic and International Communications are Intercepted

Untargeted masses of domestic and international communications are acquired and stored in the database, regardless of their foreign intelligence value. Under the Program, on the occasions where the government follows procedures established to protect Americans' privacy (obtaining a warrant or conducting minimization by purging the record from the database), it does so only after both acquisition and analyst review.

If a government analyst reviewed the communications and determined that "it was a U.S. person inside the United States . . . that would stimulate the system to get a warrant. And that is

how the process would work." Sept. 20, 2007 McConnell Testimony at 69-70 [Vol. IV, Ex. 98, pp. 3198-99]; *see also* Turner Letter at p. 7 of attachment [Vol. II, Ex. 22, p. 1044] (referencing "NSA analysts . . . querying Agency databases" to obtain communications to or from U.S. persons). In sum, the evidence shows that the NSA seeks a warrant only after the communication is (1) initially acquired and analyzed by computers according to algorithms designed by humans; (2) placed in a government database; and (3) reviewed by an analyst.

The evidence also shows that minimization is not always used. A January 2007 interview in the *New Yorker* details a particular example in which the American author's phone call to an Egyptian source was spied upon by the government. The author notes that:

> a source in the intelligence community told me that a summary of that conversation was archived in an internal database. I was surprised, because the FISA law stated that my part of the conversation should have been "minimized"—redacted or rendered anonymous—because I am an American citizen.

Lawrence Wright, *The Spymaster: Can Mike McConnell Fix America's Intelligence Community?*, NEW YORKER at 8 (Jan. 21, 2007) [Vol. II, Ex. 25, p. 1127]. McConnell explained to the author: "You called a bad guy, the system listened, tried to sort it out, and they did an intel report because it had foreign-intelligence value. That's our mission." *Id.*

Indeed, statements made in congressional testimony by former United Nations representative John Bolton confirm that NSA willingly discloses U.S. person information obtained from intercepts. In response to a question about "whether or not [he] requested to see NSA information about any other American officials" during his tenure at the State Department, Bolton revealed that "on a number of occasions" he had "asked to know the name of the [American] person" associated with the intercepts he received.[22] *Hearing on the Nomination of John Bolton to*

[22] *See also* Mark Hosenball, *Spying: Giving Out U.S. Names*, NEWSWEEK (May 2, 2005) [Vol. II, Ex. 26, p. 1131] ("[S]ince January 2004 NSA received—and fulfilled—between 3,000 and 3,500 requests from other agencies to supply the names of U.S. citizens and officials (and citizens of other countries that help NSA eavesdrop around the world, including Britain, Canada and Australia) that initially were deleted from raw intercept reports. Sources say the number of names disclosed by NSA to other agencies during this period is more than 10,000.").

be U.S. Representative to the United Nations, S. Comm. on Foreign Relations, 109th Cong. at 65 (Apr. 11, 2005) (Pt. II) [Vol. V, Ex. 105, p. 3900].

NSA agents actually eavesdropping on conversations is not, in fact, limited to calls between Americans and non-U.S. persons.[23] According to the accounts of two separate NSA whistleblowers, the agency listened in on US citizens overseas as they called friends and family in the United States – calls of "everyday, average, ordinary Americans who happened to be in the Middle East." Brian Ross, *et al*., *Exclusive: Inside Account of U.S. Eavesdropping on Americans, U.S. Officers' "Phone Sex" Intercepted; Senate Demanding Answers*, ABC NEWS at 1 (Oct. 9, 2008) [Vol. II, Ex. 27, p.1132]. One whistleblower, David Faulk, reported that "he and others in his section of the NSA facility at Fort Gordon routinely shared salacious or tantalizing phone calls that had been intercepted, alerting office mates to certain time codes of 'cuts' that were available on each operator's computer." *Id.* at 2 [p. 1133] The other whistleblower, Adrienne Kinne, said that the NSA routinely listened on calls even when analysts knew that the participants were Americans working for international aid organizations, like the International Red Cross and Doctors Without Borders: "We knew they were working for these aid organizations. . . . They were identified in our systems. . . . And yet, instead of blocking these phone numbers we continued to collect on them." *Id*. at 3 [p. 1134]. According to Kinne:

> By casting the net so wide and continuing to collect on Americans and aid organizations, it's almost like they're making the haystack bigger and it's harder to find that piece of information that might actually be useful to somebody.…You're actually hurting our ability to effectively protect our national security.

Id.

2. Evidence of Call Records Surveillance

In addition to acquisition and analysis of international and domestic communications, as

[23] *See also* STATE OF WAR at 51-52, 54 [Vol. III, Ex. 60, pp. 1609.016-017, 1609.019] ("The NSA tries to minimize the amount of purely domestic telephone and Internet traffic among American citizens that it monitors, to avoid violating the privacy rights of U.S. citizens. But there is virtually no independent oversight of NSA's use of its new power. With its direct access to the U.S. telecommunications system, there seems to be no physical or logistical obstacle to prevent the NSA from eavesdropping on anyone in the United States that it chooses. . . . Over time, the NSA has certainly eavesdropped on millions of telephone calls and e-mail messages on American soil.")

disclosed by a May 2006 report in *USA Today*, the NSA collects "the phone call records of tens of millions of Americans, using data provided by" the nation's largest telecommunications carriers. Cauley, *NSA Has Massive Database of Americans' Phone Calls* [Vol. III, Ex. 30, pp. 1182-85].[24] The NSA obtained telecommunication companies' "'call-detail records,' a complete listing of the calling histories of their millions of customers. In addition, the NSA wanted the carriers to provide updates, which would enable the agency to keep tabs on the nation's calling habits." *Id*. at 3 [p. 1184]. "Working under contract with the NSA," the companies turned over information on the numbers dialed, time of the call, and duration of the call. *Id*. at 1 [p.1182]. The NSA then uses "the data to analyze calling patterns" in order to identify and track surveillance targets. *Id*.

(a) Statements by Government and Telecommunication Company Officials Confirm that the Program Includes Surveillance of Domestic Call-Detail Records

Multiple statements by government officials briefed on the Program confirm the existence of the call records portion of the Program. In an interview with former Senator Kit Bond on PBS' NewsHour, the Senator confirmed that that the Program included call-records surveillance:

> JIM LEHRER: . . . You're a member of the Senate Intelligence Committee. Did you know about this?
>
> SEN. KIT BOND, R-Mo.: Yes. I'm a member of the subcommittee of the Intelligence Committee that's been thoroughly briefed on this program and other programs. . . . .[25]
>
> JIM LEHRER: Excuse me, Senator Leahy, and let me just ask just one follow-up question to Senator Bond so we understand what this is about.
>
> What these are, are records. And nobody then—now, these are—but there are tens of millions of records that are in this database, right? And they say somebody, Billy Bob called Sammy Sue or whatever, and that's all it says, and then they go and try to match them with other people?

---

[24] *See also* Lichtblau & Risen, *Spy Agency Mined Vast Data Trove* at 2 [Vol. IV, Ex. 66, p. 1715] (reporting that a "former technology manager at a major telecommunications company said that since the Sept. 11 attacks, the leading companies in the industry have been storing information on calling patterns and giving it to the federal government to aid in tracking possible terrorists").

[25] *See* Letter from John D. Negroponte, Director of National Intelligence, to J. Dennis Hastert, Speaker of the U.S. House of Representatives (May 17, 2006), at 2-3 [Vol. IV, Ex. 85, p. 2770-71] (listing briefings that Sen. Bond received about the Program).

> SEN. KIT BOND: First, let me say that I'm not commenting on in any way any of the allegations made in the news story today. I can tell you about the president's program.
>
> The president's program uses information collected from phone companies. The phone companies keep their records. They have a record. And it shows what telephone number called what other telephone number.

Online NewsHour Debate: *NSA Wire Tapping Program Revealed* (PBS television broadcast, May 11, 2006) [Vol. IV, Ex. 86, p. 2778].

Similarly, former Senate Majority Leader William Frist both confirmed the existence of the Program and spoke out in its defense to CNN's Wolf Blitzer:

> BLITZER: Let's talk about the surveillance program here in the United States since 9/11. USA Today reported a bombshell this week. Let me read to you from the article on Thursday.
>
> "The National Security Agency has been secretly collecting the phone call records of tens of millions of Americans using data provided by AT&T, Verizon and BellSouth. . . ."
>
> Are you comfortable with this program?
>
> FRIST: Absolutely. Absolutely. I am one of the people who are briefed . . .[26]
>
> BLITZER: You've known about this for years.
>
> FRIST: I've known about the program. I am absolutely convinced that you, your family, our families are safer because of this particular program.

Late Edition with Wolf Blitzer, *Interview with Bill Frist; Interview with Stephen Hadley* (CNN television broadcast, May 14, 2006) [Vol. IV, Ex. 87, p. 2800]. Separately, Representative Jane Harman noted that "there is a program that involves the collection of some phone records." *The Department of Homeland Security State and Local Fusion Center Program: Advancing Information Sharing while Safeguarding Civil Liberties:* Hearing of the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment of the H. Homeland Security Comm., 110th Cong. at 8 (2007) [Vol. IV, Ex. 90, p. 2843] (statement of Rep. Jane Harman).[27]

---

[26] *See* Letter from John D. Negroponte, Dir. of Nat'l Intelligence, to J. Dennis Hastert, Speaker of the U.S. House of Representatives (May 17, 2006), at 2-3 [Vol. IV, Ex. 85, pp. 2770-71] (listing briefings received by Rep. Hastert on the Program).

[27] Rep. Harman is a member of the subcommittee that received numerous briefings on the NSA programs on at least eight occasions. Letter from John D. Negroponte, Director of National

In response to the uproar over the report by *USA Today*, the White House announced that the NSA Director, Gen. Keith Alexander, would brief the full membership of both the House and Senate Intelligence Committees on the full surveillance program including "the entire scope of NSA surveillance," not to be "limited to the program that the President has publicly acknowledged." White House Press Release, *Press Briefing by Tony Snow* at 2-3, 6 (May 17, 2006) [Vol. IV, Ex. 88, pp. 2817-18, 2824]. Following those briefings, *USA Today* reported that nineteen "[m]embers of the House and Senate intelligence committees confirm that the National Security Agency has compiled a massive database of domestic phone call records" and that "[t]he program collected records of the numbers dialed and the length of calls." Susan Page, *Lawmakers: NSA Database Incomplete*, USA TODAY at 1 (June 30, 2006) [Vol. IV, Ex. 89, p. 2831].

Further, several members of Congress spoke on the record about the Program after receiving briefings. Senator Saxby Chambliss, bemoaning BellSouth's alleged refusal to participate, opined that "[i]t probably would be better to have records of every telephone company." *Id*. at 2 [p. 2832]. According to former Senator Ted Stevens, the records program targeted long-distance, not "cross-city" or "mom-and-pop calls." *Id*. Senator Orrin Hatch, Rep. Anna Eshoo, and Rep. Rush Holt also made statements on the record acknowledging the program. *Id*. at 3 [p. 2833].

Statements by government officials evidence the NSA program to collect call records proceeded under a "business records" rationale. When former Attorney General Gonzales defended the program in response to a question about the collection of "telephone detail records from the phone companies," he said that "what was in the *USA Today* story did relate to business records" and that "[t]here are a number of legal ways, of course, that the government can have access to business records." Dept. of Justice Press Release, *Transcript of "Operation GlobalCon" Press Conference* at 7 (May 23, 2006) [Vol. IV, Ex. 82, p. 2745]. In an attempt to downplay the intrusion of privacy relative to the content surveillance program, Senator Pat Roberts (who is read in to the

---

Intelligence, to J. Dennis Hastert, Speaker of the U.S. House of Representatives (May 17, 2006), at 2-3 [Vol. IV, Ex. 85, pp. 2770-71] (listing briefings received by Rep. Harman on the Program).

Program)[28] characterized the collection of private customer call records as "business records" of the telecommunications companies. His statement to Melissa Block on National Public Radio ("NPR") provides additional confirmation of the call records portion of the Program:

> BLOCK: You're saying that you are read into it. I'm curious then if you're saying that you have had oversight directly of the program as has been reported, under which the NSA has collected millions of phone records of domestic calls.
>
> Senator ROBERTS: Well, basically, if you want to get into that, *we're talking about business records*. We're not, you know, we're not listening to anybody. This isn't a situation where if I call you, you call me, or if I call home or whatever, that that conversation is being listened to.

All Things Considered: *Senate Intelligence Chair Readies for Hayden Hearings* (NPR radio broadcast, May 17, 2006) [Vol. IV, Ex. 83, p. 2749] (emphasis added); *see also Online NewsHour Debate*: NSA Wire Tapping Program Revealed, (PBS television broadcast, May 11, 2006) [Vol. IV, Ex. 86, p. 2777] (In response to a question about the call-records program, Sen. Kit Bond replied that "any lawyer should know[] that business records are not protected by the Fourth Amendment.").[29]

---

[28] *See* Letter from John D. Negroponte, Director of National Intelligence, to J. Dennis Hastert, Speaker of the U.S. House of Representatives (May 17, 2006), at 2-3 [Vol. IV, Ex. 85, p. 2770-71] (listing briefings that Sen. Pat Roberts received about the Program).

[29] Later, in August 2007, the Administration conceded that – even if the call records portion of the Program involved "business records" – the Fourth Amendment nevertheless applied:

> QUESTION: Hi. I have a couple of points that were touched on earlier, but I'm not sure really answered. On the drift net question, you talked about both the legal requirements for reasonableness under the Fourth Amendment and also just the operational logistics of using your time efficiently. Are you -- were you speaking only of surveillance where you are acquiring content, or it's your belief that those same restrictions apply to call data and tracing of call records?
>
> SENIOR ADMINISTRATION OFFICIAL: Well, the Fourth Amendment will apply to any of our activities. I mean, nothing is exempt from the reasonableness requirement of the Fourth Amendment.

Dept. of Justice Press Release, *Transcript of Conference Call with Senior Administration Officials Regarding FISA Modernization Legislation* (Aug. 7, 2007) [Vol. III, Ex. 37, p. 1273].

In total, nine members of Congress,[30] each fully briefed on "the entire scope of NSA surveillance," White House Press Release, *Press Briefing by Tony Snow* at 2-3, 6 (May 17, 2006) [Vol. IV, Ex. 88, pp. 2817-18, 2824], have acknowledged the call records program publicly and on the record.

In addition, the statements of officials from major telecommunications firms similarly confirm the existence of the call records portion of the Program. As noted in *Hepting v. AT&T*, Qwest has unequivocally confirmed requests by the government for "private telephone records of Qwest customers," which Qwest refused after learning that it would not be provided with any lawful authority permitting such access. *Hepting v. AT&T,* 439 F. Supp. 2d 974, 988 (N.D. Cal. 2006); *Full Statement From Attorney Of Former Qwest CEO Nacchio,* WALL ST. J. ONLINE (May 12, 2006) [Vol. IV, Ex. 91, p. 2854]. According to Joseph Nacchio, the former "Chairman and CEO of Qwest [who] was serving pursuant to the President's appointment as the Chairman of the National Security Telecommunications Advisory Committee," Qwest's refusal to comply was based on a "disinclination on the part of the authorities to use any legal process" in support of the request. *Id.*

Verizon Wireless admitted, through a statement by a Regional President, Kelly Kurtzman, broadcast in April 2007, that the company was asked by the government to hand over private phone records:

> LEE HOCHBERG: [A]fter 9/11, the Bush administration asked phone companies for billions of private phone records.
>
> Federal law forbids turning them over without a court order, but most phone companies did so anyway. Verizon's landline division was hit with a $50 billion consumer lawsuit for doing so. Verizon Wireless emphasizes it withheld its phone records.
>
> KELLY KURTZMAN: Absolutely, absolutely. We were asked, but we said, no, we would not give that information, again, you know, trying to protect the privacy of our customers. We take that very seriously.

[30] As noted above, the nine members are: Sens. Kit Bond, William Frist, Saxby Chambliss, Ted Stevens, Orrin Hatch, Pat Roberts, and Reps. Jane Harman, Anna Eshoo, and Rush Holt. *See supra* at 19-22.

Transcript of Online NewsHour: New Cell Phone Technology Can Track Users at 3 (PBS television broadcast, April 11, 2007) [Vol. IV, Ex. 92, p. 2858].

Thus, statements by government officials and by telecommunications executives confirm the existence of the call records portion of the Program.

(b) The Program Uses Domestic Call-Detail Records to Analyze Americans' Communication Patterns for Targeting and Investigation

The NSA uses the call-detail records acquired from the major telecommunications carriers to analyze the communications patterns of Americans in order to locate and target suspects for further surveillance and investigation.

As Secretary Chertoff confirmed, one "technique of electronic surveillance" employed under the Program includes "gathering information about who calls whom." Kondracke, *NSA Datamining Is Legal, Chertoff Says* at 3 [Vol. IV, Ex. 69, p. 1754]. Likewise, CBS News' Gloria Borger reported that Senator Roberts stated that "the NSA was looking at . . . the pattern of phone calls." Gloria Borger, *Congress to Be Briefed on NSA*, CBS/AP at 1 (May 16, 2006) [Vol. IV, Ex. 84, p. 2752]; *see also* Eric Lichtblau & Scott Shane, *Bush Is Pressed Over New Report on Surveillance*, N.Y. TIMES at 1(May 12, 2006) [Vol. II, Ex. 16, p. 728] (noting that, according to one government official, the NSA required access to "all the calls or most of them" in order to track the contacts of individuals).[31]

The database of call-detail records provides NSA with a window into the "existence, timing, and frequency of communications between persons" within the United States. *See* Declaration of J. Kirk Wiebe ("Wiebe Decl.") at ¶ 10 [Vol. VII, Ex. 120, p. 5092]. Indeed, for the

[31] *See also* Shane Harris, *NSA Spy Program Hinges on State-of-the-Art Technology*, NAT'L J. at 2 (Jan. 20, 2006) [Vol. IV, Ex. 81, p. 2722] ("One telecom executive told *National Journal* that NSA officials approached him shortly after the 9/11 attacks and insisted, to the point of questioning his company's patriotism, that executives hand over the company's 'call detail records.' Those documents, known as CDRs, trace the history of every call placed on a network, including a call's origin and destination, the time it started and ended, how long it lasted, and how it was routed through the network. Having wholesale access to many companies' records would, in theory, give the NSA a picture of telecom usage across the country.").

NSA, "a person's associations and the persistence of that association with other persons" is often "of greater relevance to a determination" that a person should be a target of investigative interest than "the actual words used in a series of communications." *Id*. at ¶ 4 [p. 5090]; *see also* Sept. 20, 2007 McConnell Testimony at 80 [Vol. IV, Ex. 98, p. 3209] (communications records provide "process for how you would find something you might be looking for. . . [t]hink of it as a roadmap"); *see also* Lichtblau & Risen, *Spy Agency Mined Vast Data Trove* at 2 [Vol. IV, Ex. 66, p. 1715] (quoting one telecom official saying, "If they get content, that's useful to them too, but the real plum is going to be the transaction data and the traffic analysis. . . Massive amounts of traffic analysis . . . [are] used to identify lines of communication that are then given closer scrutiny").

C. Evidence that AT&T Participated in the Program

The government could not and did not act alone. White House Press Release, *Statement by the Press Secretary on FISA* (Feb. 25, 2008) [Vol. II, Ex. 28 p. 1136] ("[T]he cooperation of private entities in our intelligence operations is not ancillary - it is integral to our operations and critically essential. As Director McConnell has explained, there would be no effective surveillance without the cooperation of private partners."); *see also* Sept. 20, 2007 McConnell Testimony at 13 [Vol. IV, Ex. 98, p. 3142] (The "Intelligence Community often needs the assistance of the private sector to protect the Nation. We simply cannot go alone.").

Major U.S. telecommunications companies, including AT&T, are assisting the NSA with all aspects of the Program. Chris Roberts, *Transcript: Debate On The Foreign Intelligence Surveillance Act*, EL PASO TIMES (Aug. 22, 2007) at 2 [Vol. IV, Ex. 94, p. 3017] (quoting former DNI McConnell saying "[U]nder the president's program, the terrorist surveillance program, the private sector had assisted us. Because if you're going to get access you've got to have a partner")

1. Evidence of AT&T's Collaboration with the Communications Acquisition Aspect of the Program

AT&T maintains domestic telecommunications facilities over which millions of Americans' telephone and Internet communications pass every day. Klein Decl. ¶ 7 [Vol. VII, Ex. 115, p. 4717]; *see generally The AT&T Advantage, First Quarter 2004* [Vol. IV, Ex. 70, pp. 1756-

57]; *SBC Investor Briefing*, January 31, 2005, No. 246 [Vol. IV, Ex. 71, pp. 1759-62]. These facilities allow for the transmission of interstate and foreign electronic voice and data communications by the aid of wire, fiber optic cable, or other like connection between the point of origin and the point of reception. Klein Decl. ¶ 7 [Vol. VII, Ex. 115, p. 4717].

AT&T provided the NSA with access to these communications facilities. Former AT&T technician Mark Klein has provided the Court with detailed evidence proving that AT&T has been collaborating with the NSA in the surveillance of the international and domestic communications of millions of Americans. *See* Section II(B)(1)(a), *supra* at 6-9. James Russell, AT&T's Managing Director-Asset Protection, has confirmed that Klein's declaration and the AT&T documents Klein attached accurately describe AT&T's Internet network, AT&T's San Francisco communications facility, the location of specific equipment within the San Francisco facility, and the interconnection points of AT&T's Internet network with the networks of other communications carriers. Declaration of James W. Russell ("Russel Decl.") ¶¶ 1-2, 4-7 [Vol. VII, Ex. 117, p. 5071] (filed under seal at Dkt. #84-2). Russell confirmed the conclusion that the exhibits to the Klein Declaration are authentic AT&T documents that provide "detailed schematics of network wiring configurations that are uniform across AT&T locations and that are used by AT&T to cross-connect and split fiber cables" and that "identif[y] the manufacturer and name of many pieces of equipment used by AT&T." *Id*. ¶ 7.

The Klein evidence demonstrates that the NSA controlled the surveillance configuration described in those documents. Klein's account begins around January 2003, when the manager of his facility advised him that the NSA was coming to interview another colleague for a "special job." Klein Decl. ¶ 10 [Vol. VII, Ex. 115, p. 4718]. The "special job" was to install equipment in a high-security room AT&T was building at its Folsom Street Facility in San Francisco. *Id.* ¶ 10-14 [p. 4718]. The NSA supervised the construction and outfitting of the room, which came to be known as the "SG3 Secure Room." *Id.* ¶ 12 [p. 4718]. Klein personally saw the room when it was under construction, and, at one point, entered the room briefly after it was fully operational. *Id.* ¶ 12, 17 [pp. 4718, 4719].

In October 2003, AT&T transferred Klein to the Folsom Street Facility. *Id.* ¶ 15 [p. 4718]. Although AT&T entrusted Klein with keys to every other door at the Folsom Street Facility, he did not have access to the SG3 Secure Room. *Id.* ¶ 17 [p. 4719]. No AT&T employee was allowed in the secret room without NSA security clearance. *Id*. Klein recounts one event that underscores the secrecy and "extremely limited access to the SG3 Secure Room": A large industrial air conditioner in the room began "leaking water through the floor and onto . . . equipment downstairs." *Id.* ¶ 18 [p. 4719]. AT&T maintenance personnel were not allowed to enter to fix the leak—or even to triage and prevent water damage to other portions of the facility. *Id*. Despite the "semi-emergency," AT&T waited days for an employee with NSA clearance to provide service. *Id*.

Plaintiffs' expert J. Scott Marcus confirmed "Mr. Klein's allegation that the room described was a secure facility, intended to be used for purposes of surveillance on a very substantial scale." Marcus Decl. ¶ 6 [Vol. VII, Ex. 116, p. 4747]. He "conclude[d] that AT&T has constructed an extensive—and expensive—collection of infrastructure that collectively has all the capability necessary to conduct large scale covert gathering of IP-based communications information[.]" *Id*. ¶ 38 [p. 4752]. "Given the probable cost of these configurations," and an absence of "commercial reason[s], or combination of commercial reasons" warranting the configuration, Marcus determined it was "highly probable" the configuration was funded, and used, by the U.S. government. *Id*. ¶ 46 [p. 4755].

Accordingly, the Klein Declaration and accompanying exhibits and the Marcus Declaration – coupled with the confirmation provided by the Russell Declaration – show that AT&T has built the capability necessary to conduct large-scale covert surveillance of electronic communications, and is providing the NSA with direct access to this capability as part of its ongoing collaboration with the government's warrantless surveillance Program.

2. Evidence of AT&T's Participation in the Call-Detail Records Aspect of the Program

The government also acquired call-detail records from AT&T without proper legal authorization. At a 2006 hearing before the Senate Judiciary Committee, Edward Whitacre, CEO of

AT&T, responded to a question on the call-detail records aspects of the Program by saying "if it's legal, we do it." *The AT&T And Bellsouth Merger: What Does It Mean For Consumers?:* Hearing before the Subcomm. on Antitrust, Competition Policy and Consumer Rights of the S. Comm. on the Judiciary, 109th Cong. at 13 (June 22, 2006) [Vol. V, Ex. 106, p. 3926].

In 2007, when responding to the House Energy & Commerce Committee, AT&T wrote that "the President possesses independent authority to request intelligence assistance pursuant to his" Article II powers. Letter from Wayne Watts, Senior Executive Vice President and General Counsel, AT&T, to Reps. John Dingell, Edward Markey and Bart Stupak, at 5 (Oct. 12, 2007) [Vol. IV, Ex. 101, p. 3476]. AT&T opined it would be legal for the government to "request various forms of intelligence assistance from the private sector pursuant to Executive Order 12333 and/or the President's Article II powers upon which that Order rests." *Id*; *see also Hepting v. AT&T,* 439 F.Supp.2d at 993 ("Hence, it appears AT&T helps the government in classified matters when asked and AT&T at least currently believes, on the facts as alleged in plaintiffs' complaint, its assistance is legal.").[32] Thus, it appears AT&T provides intelligence assistance when requested by the Executive, even if it violates FISA, the Wiretap Act, or the Stored Communications Act.

III. THE EVOLUTION OF THE PROGRAM OVER TIME

This section summarizes several significant events in the history of the Program. In March 2004, the legal theories that purported to support the Program became more widely known within the Administration, leading to very serious disagreements, and nearly causing the resignation of several senior officials. Later, in January 2007, the Program was purportedly authorized by the Foreign Intelligence Surveillance Court ("FISC") (though the operations remained unchanged), until the FISC reconsidered and found the Program illegal a few months later. In 2007 and 2008, Congress then passed new legislation relating to electronic surveillance. However, despite various changes in the Program's legal underpinnings, the Program remains in operation.

[32] *See also* Page, *Lawmakers: NSA Database Incomplete* [Vol. IV, Ex. 89, p. 2831] (reporting that "[f]ive members of the intelligence committees said they were told by senior intelligence officials that AT&T participated in the NSA domestic calls program").

A. Origins of the Program

The Program reflects a goal of the NSA presented to the incoming Bush administration in December 2000. According to the NSA, "[t]he volumes and routing of data make finding and processing nuggets of intelligence information more difficult. To perform both its offensive and defensive mission, NSA must 'live on the network.'" National Security Agency, *Transition 2001* at 31 (December 2000) [Vol. I, Ex. 4, p. 214]. Moreover, the NSA asserted it would be "a powerful and permanent presence on a global telecommunications infrastructure where protected American communications and targeted adversary communications will coexist." *Id*.; *see also* Remarks by Gen. Michael Hayden, *Address to the National Press Club*, Washington, D.C. (Jan. 23, 2006) [Vol. IV, Ex. 73, p. 1800] ("[T]argeted communications. . . coexisted out there in a great global web with your phone calls and my e-mails.").

But FISA stood as an obstacle to accomplishing this goal.[33] In 2000, the NSA acknowledged that 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

---

[33] John Yoo later explained why FISA was not sufficient for the Program's dragnet interception:

> [U]nder existing laws like FISA, you have to have the name of somebody, have to already suspect that someone's a terrorist before you can get a warrant. You have to have a name to put in the warrant to tap their phone calls, and so it doesn't allow you as a government to use judgment based on probability to say: "Well, 1 percent probability of the calls from or maybe 50 percent of the calls are coming out of this one city in Afghanistan, and there's a high probability that some of those calls are terrorist communications. But we don't know the names of the people making those calls." You want to get at those phone calls, those e-mails, but under FISA you can't do that.

PBS Frontline, *Spying on the Homefront*, Interview with John C. Yoo at 4 (Jan. 10, 2007) [Vol. I, Ex. 10, p. 394]; *see also* BUSH'S LAW at 143-44 [Vol. I, Ex. 1, p. 3.008-009] (discussing reasons for evading FISA); Kondracke, *NSA Data Mining is Legal, Necessary, Chertoff Says* at 1 [Vol. IV, Ex. 69, p. 1753] (According to Chertoff "getting an ordinary FISA warrant is 'a voluminous, time-consuming process' and 'if you're culling through literally thousands of phone numbers . . . you could wind up with a huge problem managing the amount of paper you'd have to generate.'"); STATE OF WAR 48 [Vol. III, Ex. 60, p. 1609.013] ("Administration officials say that one reason they decided not to seek court-approved search warrants for the NSA operation was that the volume of telephone calls and e-mails being monitored was so big that it would be impossible to get speedy court approval for all of them.").

government for such intelligence and the protection of the rights of U.S. persons," and FISA "codified this balancing." OIG PSP Report at 5 [Vol. III, Ex. 33, p. 1201]. However, shortly after the attacks of September 11, "FISA ceased to be an operative concern" for the NSA. Binney Decl. ¶ 5 [Vol. VII, Ex. 118, p. 5073]. Consequently, President Bush authorized the NSA to "conduct electronic surveillance within the United States without an order from the FISC[.]" *Id*.; *see also* Sept. 20, 2007 McConnell Testimony [Vol. IV, Ex. 98, p. 3213] ("[T]he original program that the President was operating" was unlawful in "the framework of FISA," while reserving judgment on the Article II argument).

As Gen. Hayden put it, the Program "is a more . . .'aggressive' program than would be traditionally available under FISA." *Press Briefing by Att'y Gen. Alberto Gonzalez and Gen. Michael Hayden, Principal Dep. Dir. for Nat'l Intelligence* (Dec. 19, 2005) (included as an attachment to March 2006 RJN) [Vol. V, Ex. 104, p. 3594]. This is so, in part, because "[t]he trigger is quicker and a bit softer than it is for a FISA warrant." Remarks by Gen. Michael Hayden, *Address to the National Press Club*, Washington, D.C. (Jan. 23, 2006) [Vol. IV, Ex. 73, p. 1802]. However, as the government candidly admitted, FISA requires "a court order before engaging in this kind of surveillance . . . unless otherwise authorized by statute or by Congress." *Press Briefing by Att'y Gen. Alberto Gonzalez and Gen. Michael Hayden, Principal Dep. Dir. for Nat'l Intelligence* (Dec. 19, 2005) (included as an attachment to March 2006 RJN) [Vol. V, Ex. 104, p. 3594].

The Program admittedly operated "in lieu of" court orders or other judicial authorization, *Press Briefing by Att'y Gen. Alberto Gonzalez and Gen. Michael Hayden, Principal Dep. Dir. for Nat'l Intelligence* (Dec. 19, 2005) (included as an attachment to March 2006 RJN) [Vol. V, Ex. 104, p. 3594]; *see also Proposed FISA Modernization Legislation*: Hearing before the S. Select Comm. on Intelligence, 110th Cong. at 36 (May 1, 2007) [Vol. II, Ex. 12, p. 696] (Testimony of Benjamin Powell, General Counsel, Office of the Dir. of Nat'l Intelligence) (Surveillance that was "done under the president's authorization and the president's authority were not done pursuant to

FISA or attorney general emergency authorizations by which after 72 hours you would go to the FISA Court.").

Even in the absence of judicial authorization, neither the President nor Attorney General approved the specific interceptions; rather, the decision to listen or read particular communications was made by intelligence analysts. Remarks by Gen. Michael Hayden, *Address to the National Press Club*, Washington, D.C. (Jan. 23, 2006) [Vol. IV, Ex. 73, p. 1809] (The only review process is authorization by an NSA "shift supervisor" before directly reviewing a particular individuals' communication); *see also The Terrorist Surveillance Program and FISA*: Hearing of the Subcomm. on the Constitution, Civil Rights, and Civil Liberties, H. Comm. on the Judiciary, 110th Cong. at 2 (June 7, 2007) [Vol. II, Ex. 13 p. 706] (Statement of Steven G. Bradbury, Principal Deputy Asst. Att'y Gen., Office of Legal Counsel, Dept. of Justice) ("Highly trained intelligence professionals made the initial decision to target communications for interception.").

While President Bush ultimately signed the Program Orders authorizing the Program, Vice President Cheney and the legal counsel to the Office of the Vice President, David Addington, guided the program's expansion and development.[34] Addington "was the chief legal architect [of the Program] . . . He and the vice president had abhorred FISA's intrusion on presidential power ever since its enactment in 1978. After 9/11 they and other top officials in the administration dealt with FISA the way they dealt with other laws they didn't like: They blew through them in secret based on flimsy legal opinions that they guarded closely so no one could question the legal basis for the operations." JACK L. GOLDSMITH,[35] THE TERROR PRESIDENCY: LAW AND JUDGMENT INSIDE THE BUSH ADMINISTRATION 181 (W. W. Norton 2007) ("THE TERROR PRESIDENCY") [Vol. I, Ex. 9, p 390.017].

[34] *See also* BARTON GELLMAN, ANGLER: THE CHENEY VICE PRESIDENCY 282 (PENGUIN PRESS 2008) [Vol. I, Ex. 8, p. 387.007] ("[I]t was Addington who wrote [the Program Orders], defining the reach of warrantless intrusion into the lives of Americans."); BUSH'S LAW at 144-147 [Vol. I, Ex. 1, pp. 3.009-012] (discussing origins of the Program).

[35] Goldsmith was the Assistant Attorney General for the Office of Legal Counsel in the Department of Justice from October 2003 to July 2004. OIG PSP Report at 19 [Vol. III, Ex. 33, p. 1215].

The President signed the initial Program Order on October 4, 2001, and the Program began on October 6, 2001.[36] OVP Subpoena Response [Vol. I, Ex. 3, p. 175 - 77]; Hayden Hearing at 62 [Vol. I, Ex. 2, p. 65]. The President renewed his October 4, 2001 order at least 30 times, approximately every 45 days. OIG PSP Report at 6 [Vol. III, Ex. 33, p. 1202]; OVP Subpoena Response [Vol. I, Ex. 3, p. 175 - 77]. Each Program Order – with one notable exception – was certified as to "form and legality" by the Attorney General. OIG PSP Report at 7, 11 [Vol. III, Ex. 33, p. 1203, 1207]. While not required, and of no legal significance, the Attorney General's certification helped give the "program a sense of legitimacy" and was "important [for] the cooperating private sector personnel [to] know that the Attorney General had approved the program." *Id*. at 7 [p. 1203]. The Attorney General certified the first Program Order on the "same day that he was read into the program." *Id.* at 11 [p. 1207]. The Program Orders were also accompanied by threat assessments that "documented intelligence assessments of the terrorist threats to the United States and to U.S. interest abroad." *Id*. at 7 [p. 1203].

"Knowledge of the [Program] was strictly controlled and limited at the express direction of the White House." *Id*. at 16 [p. 1212]. This excessive secrecy "created several problems," including an inability for DOJ officials to adequately review the Program's "legality during the earliest phase of the [P]rogram's operation." *Id*. Members of Congress were not informed until October 25, 2001 – nearly a month after the Program's initiation. *Id*. Even then, only four members of Congress were provided with information about the Program. *Id*. Despite FISA's requirement that electronic surveillance be performed pursuant to an order from the Foreign Intelligence Surveillance Court, no member of the Court was informed of the Program for nearly three months; then, "[f]rom January 2002 to January 2006, only FISC Presiding Judge Royce Lamberth, followed by Presiding Judge Colleen Kollar-Kotelly, were read into the" Program. *Id*. at 17 [p. 1213].

John Yoo, then a Deputy Assistant Attorney General in DOJ's Office of Legal Counsel

[36] *See also* BUSH'S LAW at 142 [Vol. I, Ex. 1, p. 3.007] (Prior to the official inception of the Program, "[w]ithin hours and days of the attacks, the NSA began ratcheting up its unmatched spyware, with the help of the U.S. telecom giants, to pore through vast amounts of communications flowing into and out of Afghanistan.")

(OLC), was responsible for "drafting the first series of legal memoranda supporting the [P]rogram." *Id*. at 10 [p. 1206].[37] "Yoo was the only OLC official 'read into' the [Program] from the program's inception in October 2001 until Yoo left DOJ in May 2003." *Id*. The first OLC opinion directly addressing the legality of the Program was not drafted until nearly a month after the Program was authorized on November 2, 2001. *Id*. at 11 [p. 1207]. Yoo's legal memoranda was later criticized for its incomplete analysis of FISA, *id*. at 12 [p. 1208]; its failure to address *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952), "a leading case on the distribution of government powers between the Executive and Legislative Branches," *id*. at 13 [p. 1209]; and for failing to "accurately describe the scope of [Program surveillance] activities." *Id*.

Yoo drafted a subsequent memo in October 2002, which largely "reiterated the same basic analysis contained in" the original OLC memorandum. *Id*. at 13. The OIG report "concluded that it was extraordinary and inappropriate that a single DOJ attorney . . . was relied upon to conduct the initial legal assessment of the [Program], and that the lack of oversight and review of Yoo's work . . . contributed to a legal analysis of the [Program] that at a minimum was factually flawed." *Id*. at 30 [p. 1226]. Ultimately, DOJ officials determined that Yoo's memoranda "did not provide a basis for finding that [all Program] activities were legal." *Id*. at 22 [p. 1218].

B. March 2004 Administration Revolt Over Illegal Surveillance

After Yoo's departure from OLC in May 2003, the legality of certain aspects of the Program became the source of "major disagreement" between DOJ officials and the White House, nearly leading to the resignation of many high-ranking DOJ officials.[38] *Id*. at 36 [p. 1232]. In

---

[37] It was David Addington and then-White House Counsel Alberto Gonzales that assigned John Yoo to prepare the Program's legal opinions. BUSH'S LAW at 156 [Vol. I, Ex. 1, p. 3.021]; ANGLER at 283 [Vol. I, Ex. 8, p. 387.008].

[38] *See also* Dan Eggen & Joby Warrick, *Data Mining Figured In Dispute Over NSA, Report Links Program to Gonzales Uproar*, WASH. POST (July 29, 2007) at 2 [Vol. III, Ex. 41, p. 1296] ("One source familiar with the NSA program said . . . that there were widespread concerns inside the intelligence community in 2003 and 2004 over how much Internet and telephone data mining could occur, as well as about the NSA's direct intercepts of communications without court approval."); BUSH'S LAW AT 178 [Vol. I, Ex. 1, p. 3.043] ("What the NSA was casting as a carefully targeted surveillance operation struck some officials as a vast data mining operation run amok, with the NSA combing through vast volumes of 'meta-data' to trace and analyze phone and e-mail traffic across the United States.").

March 2004, when the Program's authorization "was set to expire, the Department of Justice, under Acting Attorney General James Comey, refused to give its approval to the reauthorization of the order because of concerns about the legal basis of certain of these NSA activities." Letter from Alberto R. Gonzales, Att'y Gen. of U.S., to Sen. Patrick Leahy, Chairman, S. Comm. on the Judiciary at 1 (Aug. 1, 2007) [Vol. V, Ex. 102, p. 3481]; *see generally* OIG PSP Report at 20-29 [Vol. III, Ex. 33, pp. 1216–25].

The dispute began when Deputy Assistant Attorney General Patrick Philbin replaced Yoo as the OLC attorney assigned to the Program. *Id*. at 20 [p. 1216].[39] By the fall of 2003, Jack Goldsmith, then head of the Justice Department's Office of Legal Counsel, and Philbin began a factual and legal review of the Program. *Id*.; *Preserving Prosecutorial Independence: Is the Department of Justice Politicizing the Hiring and Firing of U.S. Attorneys?* Hearing before the S. Comm. on the Judiciary, Part IV, 110th Cong. at 245 (May 15, 2007) [Vol. III, Ex. 56, p. 1542] ("Comey Testimony"). Goldsmith later testified that there were certain "aspects of programs related to the TSP that I could not find legal support for," describing the Program as "a legal mess. It was the biggest legal mess I've ever encountered." *Preserving the Rule of Law in the Fight Against Terror:* Hearing before the S. Comm. on the Judiciary, 110th Cong. 7 (Oct. 2, 2007) [Vol. III, Ex. 42, p. 1307] (testimony of Jack Goldsmith); *see also* THE TERROR PRESIDENCY AT 180-82 [Vol. I, Ex. 9, pp. 390.016-18].

On Tuesday, March 9, 2004, Comey orally advised Administration officials that he saw no legal basis for certain aspects of the Program. OIG PSP Report at 24 [Vol. III, Ex. 33, p. 1220]; *see also* Comey Testimony at 246, 248 [Vol. III, Ex. 56, pp. 1543, 1545].[40] At the time, Comey was

---

[39] Philbin, who was read into the Program in mid-2003, was concerned because "[o]n its face, the program violated two felony statutes forbidding electronic surveillance without a warrant [and the] specified exceptions in those statutes did not apply." ANGLER at 288 [Vol. I, Ex. 8, p. 387.013].

[40] This conversation led to a heated dispute between Comey and Addington concerning Yoo's analysis and the Program's ongoing legal basis:

> 'The analysis is flawed, in fact facially flawed,' Comey said. 'No lawyer reading [Yoo's legal analysis] could reasonably rely on it.' . . . 'Well, I'm a lawyer and I did,' Addington said, glaring at Comey. 'No *good* lawyer,' Comey said.

the Acting Attorney General, because Attorney General John D. Ashcroft was recovering from surgery at George Washington University Hospital. OIG PSP Report at 21, 24 [Vol. III, Ex. 33, p. 1217, 1220]; *see also* Comey Testimony at 250 [Vol. III, Ex. 56, p. 1547].[41] Despite the urging of White House officials, Comey would not sign off on the legality of the Program. Comey Testimony at 224 [Vol. III, Ex. 56, p. 1521]; *see also* OIG Gonzales Report at 9 [Vol. I, Ex. 7, p. 364].

On March 10, 2004, "Gonzales and other White House and intelligence agency officials, including the Vice President and NSA Director Michael Hayden, convened an 'emergency meeting' in the White House Situation Room with" Congress's Gang of Eight.[42] OIG Gonzales Report at 9 [Vol. I, Ex. 7, p. 364]; *see also* Letter from John D. Negroponte, Dir. of Nat'l Intelligence, to J. Dennis Hastert, Speaker of the U.S. House of Representatives (May 17, 2006) at 2-3 [Vol. IV, Ex. 85, p. 2770-71] (listing congressional participants). Accounts of this meeting differ significantly. OIG PSP Report at 23 n. 16 [Vol. III, Ex. 33, p. 1219] (noting Gonzalez believed "the consensus of congressional leaders was that the [P]rogram should continue," but Rep. Pelosi, who attended the meeting, issued a statement that "'she made clear [her] disagreement with what the White House was asking' concerning the [P]rogram."). Gonzales wrote notes concerning this meeting, which "were reviewed by two NSA officials" in conjunction with a 2008 investigation into Gonzalez's mishandling of classified material. OIG Gonzales Report at 10 n. 14 [Vol. I, Ex. 7, p. 365]. "The NSA officials determined that 3 of 21 paragraphs in the notes contain SCI information about the NSA surveillance program, 1 paragraph contains SCI information about signals intelligence, and the remaining paragraphs are unclassified." *Id*.

ANGLER at 296 [Vol. I, Ex. 8, p. 387.021] (emphasis in original).

[41] *See also* ANGLER at 302-307 [Vol. I, Ex. 8, p. 387.027-32]; BUSH'S LAW at 180 [Vol. I, Ex. 1, p. 3.045].

[42] The Gang of Eight refers to congressional leadership, including the leaders of each of the two parties from each of the two houses of Congress and the chairs and ranking members of the intelligence committees of each of the two houses of Congress. *See* http://en.wikipedia.org/wiki/Gang_of_eight.

On the night of March 10, 2004, Gonzales and White House Chief of Staff Andrew Card attempted to circumvent Comey's refusal to authorize the Program, and sought Ashcroft's certification while he was recuperating from emergency surgery in the hospital. OIG PSP Report at 24 [Vol. III, Ex. 33, p. 379]; Comey Testimony at 215-17 [Vol. III, Ex. 56, pp. 1512-1514]. After learning that Gonzalez and Card were going to visit Ashcroft, Comey raced to the hospital and alerted members of his staff and FBI Director Mueller to come to the hospital to "witness [the] condition of [the] AG." OIG PSP Report at 24 [Vol. III, Ex. 33, p. 1220]. The OIG PSP Report describes the encounter in detail:

> Gonzales and Card entered Ashcroft's hospital room at 7:35 p.m., according to the FBI agent's notes. The two stood across from Mrs. Ashcroft at the head of the bed, with Comey, Goldsmith, and Philbin behind them. Gonzales told the DOJ OIG that he carried with him in a manila envelope the March 11, 2004, Presidential Authorization for Ashcroft to sign. According to Philbin, Gonzales first asked Ashcroft how he was feeling and Ashcroft replied, "Not well." Gonzales then said words to the effect, "You know, there's a reauthorization that has to be renewed. . . ." Gonzales told us that he may also have told Ashcroft that White House officials had met with congressional leaders "to pursue a legislative fix."
>
> Comey testified to the Senate Judiciary Committee that at this point Ashcroft told Gonzales and Card "in very strong terms" about his legal concerns with the [Program], which Comey testified Ashcroft drew from his meeting with Comey about the program a week earlier.

Id. at 25 [p. 1221].[43]

When Gonzales testified about the hospital incident in July 2007, he refused to say that former Attorney General Ashcroft had approved the Program for the first two years, despite heavy questioning. Instead, Gonzales testified that "from the inception, we *believed* that we had the approval of the attorney general of the United States for these activities, these particular activities."

---

[43] *See also* ANGLER at 302-303 [Vol. I, Ex. 8, p. 387.027-28]; BUSH'S LAW at 180-181 [Vol. I, Ex. 1, p. 3.045-46]. Instead of signing the Program Order, "Ashcroft gave a lucid account of the reasons that Justice had decided to withhold support. And then he went beyond that. Ashcroft said he never should have certified the program." ANGLER at 304 [Vol. I, Ex. 8, p. 387.029]; BUSH'S LAW at 182 [Vol. I, Ex. 1, p. 3.047]. According to Comey, "Ashcroft specified a list of facts, and a list of legal concerns, that the secrecy rules had prevented him from discovering. Had he known them, he said, he would have withheld his signature before." ANGLER at 459 [Vol. I, Ex. 8, p. 387.052].

Oversight of the Department of Justice: Hearing before the S. Comm. on the Judiciary, 110th Cong. 33-35 (July 24, 2007) [Vol. III, Ex. 45, pp. 1414-17] (emphasis added). Because Ashcroft had relied entirely on Yoo's incomplete description of the Program when certifying the previous Program Orders, Ashcroft believed his previous certifications were "based on a misimpression of those activities." OIG PSP Report at 26 n. 17 [Vol. III, Ex. 33, p. 1222].

Despite the conclusion by the Department of Justice that the Program could not be legally supported, President Bush nevertheless reauthorized the Program on March 11, 2004. *Id*.; Comey Testimony at 218-19 [Vol. III, Ex. 56, pp. 1515-16]. Because the Attorney General refused to certify the Program as to form and legality, the "March 11 Authorization was certified by White House Counsel Gonzales." OIG PSP Report at 26 [Vol. III, Ex. 33, p. 1222]. The March 11 Authorization differed markedly from prior authorizations in three ways:

> It explicitly asserted that the President's exercise of his Article II Commander-in-Chief authority displaced any contrary provision of law, including FISA. It clarified the description of [the Program] to address questions regarding whether such activities had actually been authorized explicitly in prior Authorizations. It also stated that in approving the prior Presidential Authorizations as to form and legality, the Attorney General previously had authorized the same activities now being approved under the March 11 Authorization.

Id. This last provision was "removed from future Authorizations after Ashcroft complained to Gonzales that the statement was 'inappropriate.'" *Id*. at 26 n. 17 [p. 1222].

As a result of the reauthorization without DOJ approval, about "two dozen Bush appointees," including Acting Attorney General Comey and FBI Director Mueller, were prepared to resign. *See* Comey Testimony at 250 [Vol. III, Ex. 56, p. 1547] (partial list of people prepared to resign); OIG PSP Report at 27 [Vol. III, Ex. 33, p. 1223].[44] Despite the illegality of the Program, no officials resigned and Comey did not direct "the FBI to cease cooperating with the NSA in conjunction with the [P]rogram." OIG PSP Report at 28 [Vol. III, Ex. 33, p. 1224].

[44] *See also* Scott Shane & David Johnston, *Mining of Data Prompted Fight Over U.S. Spying*, N.Y. TIMES at 1 (July 29, 2007) [Vol. III, Ex. 46, p. 1458] (The March "2004 dispute over the National Security Agency's secret surveillance program that led top Justice Department officials to threaten resignation involved computer searches through massive electronic databases, according to current and former officials briefed on the program. . . . [S]uch databases contain records of the phone calls and e-mail messages of millions of Americans.")

From March 11 through March 16, 2004, the Program continued unchanged, while "an interagency working group led by OLC was convened to continue reanalyzing the legality" of the Program. *Id*. On March 17, 2004, the President decided to modify certain aspects of the Program and to discontinue others that DOJ believed were legally unsupportable.[45] *Id*. at 29 [p. 1225].

In May 2004, "Goldsmith and Philbin completed an OLC legal memorandum assessing the legality of the [Program] as it was operating at that time." *Id*. The OLC memorandum asserted that the Authorization for Use of Military Force (AUMF) passed by Congress shortly after the attacks of September 11, 2001 gave the President authority to use both domestically and abroad 'all necessary and appropriate force,' including signals intelligence capabilities, to prevent future acts of international terrorism . . . ." *Id*.

C. The Transition of Certain Program Activities to Foreign Intelligence Surveillance Court Orders

From 2004 to 2007, "[c]ertain activities that were originally authorized as part of the [P]rogram have subsequently been authorized under orders issued by the Foreign Intelligence Surveillance Court (FISC)." OIG PSP Report at 30 [Vol. III, Ex. 33, p. 1226]. Included in this transition was the "interception of certain international communications that the President publicly described as [the TSP]," as well as other "[Program]-authorized activities." *Id*. "As a result of this transition, the President decided not to reauthorize these activities and the final Presidential Authorization expired on February 1, 2007." *Id*.

In 2004, the government for the first time sought an order from the FISC for "business records" under FISA. Dept. of Justice, Office of Inspector Gen, *A Review of the FBI's Use of Section 215 Orders for Business Records in 2006* at 16-17 (March 2008) [Vol. V, Ex. 108, p. 4036-37]; *see* Section II(B)(2)(a), *supra* at 22-23 (call records program operated under "business records" rationale). Government officials later disclosed these business records orders supported a "sensitive collection program." *The USA PATRIOT Act,* Hearing Before the Subcomm. on the

[45] *See also* ANGLER at 321 [Vol. I, Ex. 8, p. 387.046] (Even after modifying aspects of the Program, the Administration, in a memo issued a few days later, "reasserted the lawfulness of every element of the program," and asserted that the changes were "for strictly operational reasons, at the president's own discretion.")

Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. at 8 (Sept. 22, 2009) [Vol. V., Ex. 109, p. 4124] (testimony of Todd Hinnen, Dep. Asst. Att'y Gen.). The government's use of business records orders has caused condemnation from elected officials. Senator Richard Durbin noted that the government's reliance on business records orders "is unfortunately cloaked in secrecy. Some day that cloak will be lifted, and future generations will ask whether our actions today meet the test of a democratic society: transparency, accountability, and fidelity to the rule of law and our Constitution." *Executive Business Meeting*, S. Comm. on the Judiciary (October 1, 2009) [Vol. VI, Ex. 110, p. 4271] (Remarks of Sen. Richard Durbin). Senator Ron Wyden reiterated Senator Durbin's concerns nearly two years later:

> I have served on the Intelligence Committee for over a decade and I wish to deliver a warning this afternoon. When the American people find out how their government has secretly interpreted [the business records provision of FISA], they are going to be stunned and they are going to be angry.

157 Cong. Rec. S3372-3402, S3386 (May 26, 2011) [Vol. VI, Ex. 111, p. 4286] (Statement of Sen. Ron Wyden, On Patriot Act Reauthorization).

The interception of international communications targeting members of terrorist groups was also included in the transition to FISC orders. OIG PSP Report at 30 [Vol. III, Ex. 33, p. 1226]. In a letter to the Congress on January 17, 2007, then Attorney General Gonzales announced that a judge of the Foreign Intelligence Surveillance Court:

> issued orders authorizing the [g]overnment to target for collection international communications into or out of the United States where there is probable cause to believe one of the communicants is a member or agent of al Qaeda or an associated terrorist group. As a result of these orders, any electronic surveillance that was occurring as part of the Terrorist Surveillance Program will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court.

Letter from Alberto Gonzales, Att'y Gen. of U.S., to Sen. Patrick J. Leahy, Chairman, S. Comm. on the Judiciary, and Sen. Arlen Specter, Ranking Minority Member, S. Comm. on the Judiciary (Jan. 17, 2007) [Vol. IV, Ex. 74, p. 2451].

However, in May 2007, a second FISC judge refused to renew the January 2007 FISC orders authorizing aspects of the Program. According to the Senate Select Committee on Intelligence "[a]t the end of May 2007. . . attention was drawn to a ruling of the FISA Court. When

a second judge of the FISA Court considered renewal of the January 2007 FISA orders, he issued a ruling that the DNI later described as significantly diverting NSA analysts from their counterterrorism mission to provide information to the Court." Report on S. Rep. 110-209, *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2007*, Sen. Select Comm. on Intelligence, 110th Cong. (Oct. 26, 2007) [Vol. IV, Ex. 96, p. 3034]. The FISC order has not been made public. *In re Motion for Release of Court Records*, 526 F.Supp.2d 484 (Foreign Intel.Surv.Ct. 2007).[46]

In an August 2007 interview the *El Paso Times*, DNI McConnell said:

> [The Program] was submitted to the FISA court and the first ruling in the FISA court was what we needed to do we could do with an approval process that was at a summary level and that was OK, we stayed in business and we're doing our mission. . . . But the FISA process has a renewal. It comes up every so many days and there are 11 FISA judges. So the second judge looked at the same data and said well wait a minute I interpret the law, which is the FISA law, differently.

Chris Roberts, *Transcript: Debate On The Foreign Intelligence Surveillance Act*, EL PASO TIMES at 1 (Aug. 22, 2007) [Vol. IV, Ex. 94, p. 3016].

In a February 2008 interview, ODNI Spokesman Russ Feinstein clarified that "[d]ue to rulings from the FISA court, in a significant number of cases, the government had to get court orders for purely foreign-to-foreign communications that touched American wires." Ryan Singel, *Can the NSA Wiretap in Iraq Without A Warrant?*, WIRED NEWS (Feb. 28, 2008) [Vol. III, Ex. 51, p. 1475]. Feinstein was correcting an earlier, and broader, statement that "if a communication touches a U.S. wire, you need a court order." *Id.*

In March 2008, Assistant Attorney General for National Security Kenneth Wainstein admitted that the problem was with email communications, not phone calls. "The real concern, he said, is primarily e-mail, because 'essentially you don't know where the recipient is going to be' and so you would not know in advance whether the communication is entirely outside the United

[46] *See also* Greg Miller, *New Limits Put On Overseas Surveillance*, L.A. TIMES (Aug. 2, 2007) at 1 [Vol. III, Ex. 50, p. 1473] ("One official said the issue centered on a ruling in which a FISA court judge rejected a government application for a 'basket warrant' – a term that refers to court approval for surveillance activity encompassing multiple targets, rather than warrants issued on a case-by-case basis for surveillance of specific terrorism suspects.").

States." Ellen Nakashima & Paul Kane, *Wiretap Compromise in Works: FISA Update May Hinge On Two Separate Votes*, WASH. POST at 1 (March 4, 2008) [Vol. III, Ex. 52, p. 1478]. Indeed, e-mail surveillance constitutes the majority of the NSA's collections. Sept. 18, 2007 McConnell Testimony at 78 [Vol. II, Ex. 17, p. 811] (estimating the FISC decision effected "about two-thirds of our capability").[47]

D. The Program After the Protect America Act of 2007 and the FISA Amendments Act of 2008

In August 2007, Congress passed the Protect America Act of 2007, Pub. L. 110-55, 121 Stat. 552 ("PAA"). In September 2007, Assistant Attorney General Wainstein wrote to Chairman Silvestre Reyes that "[t]he Protect America Act does not authorize so-called 'domestic wiretapping' without a court order, and the Executive Branch will not use it for that purpose." Letter from Kenneth L. Wainstein, Asst. Att'y Gen. for Nat'l Sec., U.S. Dept. of Justice, to Rep. Silvestre Reyes, Chairman, H. Permanent Select Comm. on Intelligence (Sept.14, 2007) [Vol. III, Ex. 53, p. 1482]; *see also* Department of Justice Press Release, *Transcript of Conference Call with Senior Administration Officials Regarding FISA Modernization Legislation* (Aug. 7, 2007) at 10 [Vol. III, Ex. 37, p. 1269] ("[W]e also don't think you could direct surveillance at a large number of persons in the United States without using the FISA regime.").

Following the expiration of the PAA in early 2008, Congress passed the FISA Amendments Act of 2008 ("FAA"). Pub. L. 110-261, 122 Stat. 2436 (2008); OIG PSP Report at 31 [Vol. III, Ex. 33, p. 1227]. The FAA "authorized the government to intercept inside the United States any communications of non-U.S. persons reasonably believed to be located outside the United States, provided a significant purpose of the acquisition pertains to foreign intelligence." *Id*. at 31 [p. 1227]. Accordingly, none of the assistance alleged in the complaint was provided pursuant to the PAA or the FAA.

[47] *See also* BUSH'S LAW at 153 [Vol. I, Ex. 1, p. 3.018] ("[D]espite the public focus on phone calls, most of the NSA's intercepts—75 percent by one estimate—were e-mails.").

E. The Ongoing Operation of the Program

Despite the transition to FISC orders, the operation of the Program remains unchanged. After the FISC issued its first order, Press Secretary Tony Snow explained "[w]hat happens is that the program pretty much continues – the program continues." White House Press Release, *Press Briefing by Tony Snow* at 5 (Jan. 17, 2007) [Vol. III, Ex. 47, p. 1465]. A reporter sought clarification:

> Q: In other words, we now have a new program called --
>
> MR. SNOW: No, you have the same program it operates under, but it's really a matter of your legal authority prior to that. It was presidential order. Now, in this case, the program continues, but it continues under the rules that have been laid out by the court.

Id. Likewise, in a background briefing given on the same day, the government officials explained that the shifting authorization wouldn't cause "any significant operational impact" so the Program "continue to do everything" authorized under the prior Program. Dept. of Justice Press Release, *Transcript of Background Briefing on FISA Authority of Electronic Surveillance by Senior Justice Department Officials* at 3 (Jan. 17, 2007) [Vol. I, Ex. 6, p. 348]; *see also id.* at 6 [p. 351] ("[T]he general contours under these orders allow us to do the same thing and to target the same types of communications. . . . [T]he objectives of the program haven't changed and the capabilities of the intelligence agencies to operate such a program have not changed as a result of these orders."). Moreover, the basic legal rationale had not changed:

> I don't know that anything has changed. First of all, let me say that we continue to believe as we've always said and as we've explained at length that the President has the authority to authorize the terrorist surveillance program, that he has that authority under the authorization for the use of military force and under Article II of the Constitution. That's not changing.

Id. at 2 [p. 347]; *see also* James Risen, *Administration Pulls Back on Surveillance Agreement*, N.Y. TIMES at 1 (May 2, 2007) [Vol. III, Ex. 48, p. 1469] ("[S]enior officials, including Michael McConnell, the new director of national intelligence, said they believed that the president still had the authority under Article II of the Constitution to once again order the N.S.A. to conduct surveillance inside the country without warrants.").

Rather than limiting the untargeted acquisition of large quantities of domestic

communications, the new authorizations focused on minimization after collection. "At the [January 18, 2007, Senate Judiciary] hearing, Mr. Gonzales said the rules protected national security by allowing continued eavesdropping, but required the government to halt quickly the monitoring of people who were not found to be doing anything wrong." David Johnston & Scott Shane, *Senators Demand Details on New Eavesdropping Rules*, N.Y. TIMES (Jan. 19, 2007) [Vol. III, Ex. 49, p. 1472]; *see also Dept. of Justice Oversight*: Hearing before the S. Comm. on the Judiciary, 110th Cong. at 44 (Jan 18, 2007) [Vol. I, Ex. 11, p. 447] (Testimony of Alberto Gonzalez).

Indeed, in another series of articles in 2009, the *New York Times* revealed that the Program was again operating outside the broad limits established under the FAA. Eric Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. TIMES (April 15, 2009) [Vol. III, Ex. 38, pp. 1277-79]. The Justice Department acknowledged "there had been problems with the NSA's surveillance operation." The problems involved a "serious issue involving the NSA" concerning "significant misconduct." *Id*. at 1, 3 [pp. 1277, 1279].

The problems, which led to congressional inquiries, largely involved the "flagrant" overcollection of domestic email. Eric Lichtblau & James Risen, *E-Mail Surveillance Renews Concern in Congress*, N.Y. TIMES at 1(June 17, 2009) [Vol. III, Ex. 57, p. 1586] (quoting Rep. Rush Holt). "Because each court order could single out hundreds or even thousands of phone numbers or e-mail addresses, the number of individual communications that were improperly collected could number in the millions, officials said." *Id*. at 2 [p. 1587]. "'Say you get an order to monitor a block of 1,000 e-mail addresses at a big corporation, and instead of just monitoring those, the N.S.A. also monitors another block of 1,000 e-mail addresses at that corporation,' one senior intelligence official said. 'That is the kind of problem they had.'" *Id*. at 2-3 [pp. 1587-88].

Consistent with those reports, the FISC has held, on at least one occasion, that the Program's ongoing surveillance violated the Fourth Amendment and that surveillance conducted under the Program violated the spirit of the law. Letter from Kathleen Turner, Director of Legislative Affairs, Office of the Dir. of Nat'l Intelligence, to Sen. Ron Wyden at 1(Jul. 20, 2012) [Vol. VI, Ex. 113, p. 4609].

IV. EVIDENCE PROVIDING CONTEXT FOR GOVERNMENT ASSERTIONS ABOUT THE PROGRAM

This section summarizes the evidence that provides important context for understanding the government's assertions about the Program. This context may be useful to the Court in evaluating the government's assertion of the state secrets privilege and its statements about its activities at issue in this case. In brief, the government has used carefully parsed statements and omissions that elide or obscure the actual surveillance activities it has undertaken.

A. Use of the Term "Terrorist Surveillance Program"

Government officials have generally cabined their discussions of the Program to "the Program as described by the President," or the so-called "Terrorist Surveillance Program." *See e.g.* Gov't Br. at 3:9-12 (Dkt. # 102) ("President Bush acknowledged the existence of a program he authorized . . . later referred to as the 'Terrorist Surveillance Program.'"); Public Declaration of James R. Clapper, Director of National Intelligence ("Clapper Decl.") (Dkt. # 104) ¶ 24 ("[P]laintiffs' allegation that the NSA has indiscriminately collected the content of millions of communications sent or received by people inside the United States after 9/11 under the TSP is false."). Director Fleisch's declaration similarly discusses the Program in terms of the TSP: "Plaintiffs allege that the presidentially-authorized activities at issue in this litigation went beyond the "Terrorist Surveillance Program . . . Rather, plaintiffs allege that other intelligence activities were also authorized by the President after 9/11[.]" Declaration of Frances J. Fleisch, National Security Agency (Dkt. # 105) ¶ 3.

However, outside of this litigation, the government has repeatedly confirmed that the Program included "other intelligence activities," beyond those described as the TSP. The OIG PSP Report, on the first page, makes this clear:

> [After September 11, 2001,] the President authorized the National Security Agency (NSA) to conduct a classified program . . . As part of the NSA's classified program, *several different intelligences activities were authorized* . . . One of the activities authorized as part of the [Program] was the interception of the content of communications into and out of the United States where there was a reasonable basis to conclude that one party to the communication was a member of al-Qa'ida or related terrorist organizations. This aspect of the [Program] was publicly acknowledged and described by the President, the Attorney General, and other

> Administration officials beginning in December 2005 following a series of articles published in the New York Times. . . . The President and other Administration officials labeled the publicly disclosed interception of the content of certain international communications by the NSA as the "Terrorist Surveillance Program."

OIG PSP Report at 1 [Vol. III, Ex. 33, p. 1197] (emphasis added).

The phrase "Terrorist Surveillance Program" does not describe the entire surveillance Program or even an independent program, but rather only those aspects of the broader Program that were publicly described by the President in 2005. Letter from Att'y Gen. Alberto Gonzalez to Sen. Patrick Leahy (Aug. 1, 2007) [Vol. V, Ex. 102, p. 3481] ("[B]efore December 2005, the term 'Terrorist Surveillance Program' was not used to refer to these activities, collectively or otherwise. It was only in early 2006, as part of the public debate that followed the unauthorized disclosure and the President's acknowledgement of one aspect of the NSA activities, that the term Terrorist Surveillance Program was first used.").

Government officials have steered the public debate, and their briefing before this Court, towards the TSP, in an effort to assert that the broader Program is limited, justified, and is no longer in operation. Thus, when the government asserts the NSA has not "indiscriminately collected the content of millions of communications . . . under the TSP," Clapper Decl. ¶ 24, the government is *not* asserting that this conduct does not occur under the *broader* surveillance Program.

B. Use of the Terms "Surveillance" and "Collection"

The government regularly uses the terms "surveillance" and "collection" to describe Program activities, yet the definitions it uses for those terms are notably narrower than either the plain meaning of the term or their legal definition.

In public discussions of the Program, the government appears to exclude from the term "surveillance" instances where communications are acquired but subsequently "minimized," despite the broader legal definition of "electronic surveillance" under applicable law. *See, e.g.*, 50 U.S.C. § 1801(f). For example, the statement of White House press secretary Tony Snow displays this irregular usage:

> MR. SNOW: … the target in these conversations: a foreign individual not on U.S. soil. If that person is talking to a U.S. citizen, it does not mean that you're sitting around doing surveillance on the U.S. citizen. Furthermore, if it is a --
>
> Q But if you're surveilling a phone call, you're not just listening to the foreigner's side of the call, right?
>
> MR. SNOW: Well, yes, but on the other hand, if -- you probably understand that if somebody is just calling in and asking how his socks are at the dry cleaners, all of that personal information is combed out and, in fact, the U.S. citizen basically – you're not conducting surveillance.

White House Press Release, *Press Briefing by Tony Snow* at 2 (Aug. 8, 2007) [Vol. III, Ex. 59, p. 1606].

Similarly, the government's definition of what it means to "collect" intelligence information is notably narrow: under Department of Defense regulations, information is considered to be "collected" only after it has been "received for use by an employee of a DoD intelligence component," and "[d]ata acquired by electronic means is 'collected' only when it has been processed into intelligible form[,]" without regard to when the information was initially acquired by a surveillance device. Dept. of Defense, DOD 5240 1-R, Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons § C.2.2.1 at 15 (Dec. 1982) [Vol. II, Ex. 24, p. 1070]. Consequently, the NSA could engage in electronic surveillance of communications, within the meaning of FISA, without engaging in either "surveillance" or "collection," according to its own definitions.

Thus, when the government asserts that the NSA has not "indiscriminately collected the content of millions of communications," it does not mean that the content of millions of communications have not been subject to electronic surveillance by the government: it means only that the "content of millions of communications" have not been "processed into an intelligible form" for human review.

C. Use of the Terms "Content," "Conversations," and "Communications"

The government also expressly defines "content" in the context of its brief and in the Clapper and Fleisch Declarations in a narrow way. Gov't Br. at 22 fn. 12; Clapper Decl. ¶ 23 n.1; Fleisch Decl. ¶ 12 fn. 4. These documents define "content" to include only the "substance, meaning

or purport of a communication," as defined in 18 U.S.C. §2510(8). However, for purposes of FISA, the term "content" is defined to include: "*any information concerning the identity of the parties to such communication or the existence,* substance, purport, or meaning of that communication." 50 U.S.C. § 1801(n) (emphasis added).

For example, despite the broad definition of "content" used in FISA, the government excludes all communications records (or "metadata") from its definition of the term, as demonstrated by this statement from DNI McConnell:

> Mr. HOLT. Do you need to be able to conduct bulk collection of call detail records, metadata for domestic-to-domestic phone calls by Americans?
>
> Director MCCONNELL. *Metadata, we think of it as not content* but a process for how you would find something you might be looking for. Think of it as a roadmap.

Sept. 20, 2007 McConnell Testimony at 80 (emphasis added) [Vol. IV, Ex. 98, p. 3209].

Moreover, for purposes of the claims in this case, "content" includes email subject lines and URLs. *See* 18 U.S.C. § 2510(8); 50 U.S.C. § 1801(n). And the government has, in other contexts, admitted that information like the "subject lines" of email and the URLs of web links are the "content of communications." Dept. of Justice, Computer Crime and Intellectual Property Section, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations,* Chapter 3 (2002)) ("[t]he subject headers of e-mails are also contents.") [Vol. III, Ex. 62, p. 1631]; Dept. of Justice*, U.S. Attorneys' Manual* 9-7.500 (2003) [Vol. III, Ex. 63, p. 1640] (prohibiting the collection of URLs without prior consultation with DOJ to determine whether the URLs to be collected will constitute content). Nevertheless, when describing the Program, the government appears to exclude both subject lines and URLs from its definition of "content." For example, Gen. Hayden testified that "we do not use the content of communications to decide which communications we want to study the content of." Hayden Hearing at 50 [Vol. I, Ex. 2, p. 53]. However, in the next sentence, Hayden shows he was using a crabbed definition of "content" that excludes the subject lines of email and the URLs of web links: "in other words, when we look at the content of the communications, everything between 'hello' and 'good bye'…." *Id.*

The government has also used the terms "conversations" and "communications" in ways that obscure the Program's scope. For example, in a January 2006 speech at the National Press Club, Gen. Hayden, as the former Director of the NSA, attempted to downplay fears after the Program's initial disclosure by the *New York Times*. Hayden said:

> Let me talk for a few minutes also about what this program is not. It is not a driftnet over Dearborn or Lackawanna or Freemont grabbing conversations that we then sort out by these alleged keyword searches or data-mining tools or other devices that so-called experts keep talking about.

Remarks by Gen. Michael Hayden, *Address to the National Press Club*, Washington, D.C. (Jan. 23, 2006) [Vol. IV, Ex. 73, p. 1802]; *see also* Letter from William E. Moschella, Asst. Att'y Gen., U.S. Dept. of Justice, to Sen. Arlen Specter, Chairman, S. Comm. on the Judiciary (Mar. 24, 2006) at 4 [Vol. III, Ex. 61, p. 1614] (response to Senator Leahy's question 7).

Later, however, after the May 11, 2006 *USA Today* story brought the government's creation of a vast database of domestic calls to the attention of the American public, *see* Section II(B)(2), *supra* at 19-24, Hayden had to explain how the creation of a vast database of Americans' calls could not constitute a "drift net" of communications. Hayden backtracked from his 2006 remarks, testifying:

> [A]t key points, key points in my remarks, I pointedly and consciously downshifted the language I was using.
>
> When I was talking about a drift net over Lackawanna or Freemont or other cities, I switched from the word "communications" to the much more specific and unarguably accurate conversation.

Hayden Hearing at 50 [Vol. I, Ex. 2, p. 53]; *but see* Gorman, *NSA's Domestic Spying Grows As Agency Sweeps Up Data* at 4-5 (quoting Hayden's January 2006 remarks and then noting that "intelligence officials now say the broader NSA effort amounts to a driftnet") [Vol. IV, Ex. 95, p. 3026-27].

D. The Government's Assertions of Harm to National Security are Inconsistent With Its Actions

Throughout this litigation and the related MDL the government has asserted that the revelation of certain information would "cause exceptionally grave harm to national security." *See,*

e.g, Gov't Br. at 2:2-3. However, the record shows instances in which the government claimed harm to national security, yet later disclosed the very same in this litigation and in the broader public debate.

For example, on May 24, 2007, the government asserted that:

> Plaintiffs in these cases put directly at issue whether or not the NSA has conducted particular intelligence activities and whether or not it has done so *with the secret help of a private entity*. The disclosure of any information that would tend to confirm or deny these allegations . . . would cause exceptionally grave harm to the national security.

Public Declaration of J. Michael McConnell, Dir. of Nat'l Intelligence, No M:06-CV-1791 (May 24, 2007), ¶ 13 (Dkt. # 254-3) [Vol. IV, Ex. 77, p. 2531] (emphasis added). Likewise, in August 2007, the government stated that revealing even the "type of company" who assisted the government would result in "potentially grave harm to national security." Government's Response to Pls.' Req. for Judicial Notice, *Hepting v. AT&T*, 06-CV-17132 at 5-6 [Vol. III, Ex. 64, p. 1651-52].

Nevertheless, the government later freely disclosed both that the private sector helped with the Program and that the providers of that assistance were telecommunications companies. *See* Section II(C), *supra* at 25-29; *see also* Sept. 20, 2007 McConnell Testimony at 13 [Vol. IV, Ex. 98, p. 3142] ("It is important to keep in mind that the Intelligence Community often needs the assistance of the private sector."); White House Press Release, *Straight To The Point* (Feb. 28, 2008) [Vol. IV, Ex. 100, p. 3244] ("You cannot expect phone companies to participate if they feel like they're going to be sued."); White House Press Release, *Statement by the Press Secretary on FISA* (Feb. 25, 2008) [Vol. II, Ex. 28, p. 1136] ("[T]he cooperation of private entities in our intelligence operations is not ancillary – it is integral to our operations and critically essential."); White House Press Release, *Press Briefing by Dana Perino* (Feb. 12, 2008) [Vol. III, Ex. 32, p. 1192]; White House Press Release, *Transcript of Background Briefing by Senior Administration Officials on FISA* at 2 (Feb. 26, 2008) [Vol. II, Ex. 15, p. 721].

Likewise, in then-DNI McConnell's May 25, 2007, declaration in *Shubert v. Bush*, the government asserted that "grave harm" would result from the disclosure of "[i]nformation that may

tend to *confirm or deny* whether Verizon/MCI, AT&T, or any other telecommunications carrier has assisted the NSA with the alleged intelligence activities." Public Declaration of J. Michael McConnell, Dir. of Nat'l Intelligence, *Shubert v. Bush*, 07-CV-693 (May 24, 2007), ¶¶ 11c, 13 (Dkt. # 295-3) [Vol. IV, Ex. 78, p. 2550] (emphasis added). However, the Attorney General's later September 2008 certification in the MDL actions then denied that Verizon/MCI, AT&T, or any other telecommunications carrier has assisted the NSA with the alleged content dragnet. Public Certification of Att'y Gen. of the United States Michael Mukasey, *In re NSA Telecomm. Records Litigation*, MDL Case No. M:06-1791-VRW (Dec. 2, 2008) (Dkt. # 469-3), at 5:16-19 [Vol. III, Ex. 40, p. 1286].

Similar to the current arguments presented by the government in this case, in moving to dismiss the Verizon plaintiffs' case in 2007, the government argued "Plaintiffs' content surveillance claim in this case (as in *Hepting*) boils down to an unfounded and highly speculative allegation that they do not believe that the President authorized only a limited surveillance program directed at certain al Qaeda-related international communications." Motion to Dismiss the Verizon Master Consolidated Complaint, *In re NSA Telecomm. Records Litigation*, MDL Case No. M06-1791-VRW (N.D. Cal. 2007) (Dkt. # 254), at 3 [Vol. IV, Ex. 77, p. 2470]. Proving whether or not the President authorized more, the government asserted, would cause "grave harm." *Id*.

Nevertheless, the first page of OIG PSP Report makes clear that the President authorized "several different intelligence activities." OIG PSP Report at 1 [Vol. III, Ex. 33, p. 1197]; *see also* Letter from J. Michael McConnell, Dir. of Nat'l Intelligence, to Sen. Arlen Specter, Ranking Member, S. Comm. on the Judiciary (July 31, 2007) [Vol. IV, Ex. 93, p. 3014] (admitting that the President authorized more than a limited surveillance program directed at certain al Qaeda-related international communications).

The government also states that even "[t]he process of sorting out whether any allegation is true, party true, or wholly false, would . . . cause exceptionally grave damage to national security." Gov't Mot. at 24:15-19 (citing Fleisch Decl. ¶ 4; Clapper Decl. ¶ 3). Yet, in testimony before Congress earlier this year, when describing the capabilities of the NSA within the United States,

NSA Director General Alexander denied many of Plaintiffs' allegations. In a colloquy with Rep. Hank Johnson concerning the interception of Internet communications, General Alexander described those capabilities, stating:

> General ALEXANDER. The question is where are the e-mails, and where is NSA's coverage? I assume by your question that those e-mails are in the United States.
>
> Mr. JOHNSON. Correct.
>
> General ALEXANDER. NSA does not have the ability to [target emails based on their content] in the United States. . . . We don't have the technical insights in the United States. In other words, you have to have something to intercept or some way of doing that either by going to a service provider with a warrant, or you have to be collecting in that area. We are not authorized to collect. Nor do we have the equipment in the United States to actually collect that kind of information. . . .
>
> Mr. JOHNSON. . . . NSA has software that, quote, "searches U.S. sources for targeted addresses, locations, countries, and phone numbers, as well as watchlisted names, key words, and phrases in e-mail[]". . . . Is this true?
>
> General ALEXANDER. No, it is not. . . .
>
> Mr. JOHNSON. Does the NSA intercept Americans' cell phone conversations?
>
> General ALEXANDER. No.
>
> Mr. JOHNSON. Google searches?
>
> General ALEXANDER. No.

Fiscal Year 2013 Budget Request for Information Technology and Cyber Operations Programs, Hearing before the House Armed Services Comm., Subcomm. on Emerging Threats and Capabilities, 112th Cong. at 20 (March 20, 2012) [Vol. V, Ex. 103, p. 3505-06] (testimony of Gen. Keith Alexander, Dir. of Nat'l Security Agency). As General Alexander's testimony before Congress demonstrates, the discussion of NSA's domestic surveillance capabilities and the limits of those capabilities does not threaten harm to national security.

Similarly, a 300-page Department of Justice Office of Inspector General report described in exhaustive detail the FBI's use of so-called "exigent letters" to obtain call record information from telecommunication companies. Dept. of Justice, Office of the Inspector Gen., *A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records* at 9 (Jan. 2010) [Vol. VI, Ex. 112, p. 4324]. The FBI used these letters –

instead of National Security Letters, grand jury subpoenas, or other legal process – to obtain call records from three major telecommunication firms on subscribers and their "community of interest" or "calling circle". *Id*. at 64 – 78 [pp. 4379-93]. Thus, as the OIG's exigent letter report demonstrates, national security concerns do not preclude all discussion of an intelligence agency's procurement of call records without legal process. Moreover, multiple in-depth, substantive analyses concerning the full scope of the Program have occurred without disclosure of classified information. *See Oversight of the Department of Justice*: Hearing before the S. Comm. on the Judiciary, 110th Cong. at 67 (July 24, 2007) [Vol. III, Ex. 45, p. 1446] (noting that, when discussing the Program in John Ashcroft's hospital room, "General Ashcroft did virtually all of the talking, and he did all the talking with respect to the legal issues . . . I don't believe that he disclosed classified information in the hospital room."); *see generally* OIG PSP Report [Vol III, Ex. 33].

V. CONCLUSION

Plaintiffs respectfully request that the Court consider this Summary of Voluminous Evidence pursuant to Rule 1006, including evidence previously submitted and the new evidence submitted with the accompanying Declaration of Kurt Opsahl. This summary is offered to aid the Court by bringing together a summary of Plaintiffs' relevant evidence that the Court may consider at this stage of the litigation.

DATE: October 9, 2012

Respectfully submitted,

s/ Richard R. Wiebe

CINDY COHN
LEE TIEN
KURT OPSAHL
JAMES S. TYRE
MARK RUMOLD
ELECTRONIC FRONTIER FOUNDATION

RICHARD R. WIEBE
LAW OFFICE OF RICHARD R. WIEBE

THOMAS E. MOORE III
THE MOORE LAW GROUP

RACHAEL E. MENY
PAULA L. BLIZZARD
MICHAEL S. KWUN
AUDREY WALTON-HADLOCK
KEKER & VAN NEST LLP

ARAM ANTARAMIAN
LAW OFFICE OF ARAM ANTARAMIAN

Attorneys for Plaintiffs