IN THE 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.

No C 08-cv-4373 VRW

IN RE:

NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION

THIS DOCUMENT RELATES TO:

VIRGINIA SHUBERT, NOHA ARAFA, SARAH DRANOFF AND HILARY BOTEIN, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED,

Plaintiffs,

v

BARACK H OBAMA ET AL,

Defendants.

_____/

MDL Docket No C 06-1791 VRW

Member case No C 07-0693 VRW

ORDER

These two actions are among those filed in response to revelations in the press, beginning in December 2005, that the National Security Agency (NSA), an agency of the United States government, had carried out one or more programs involving warrantless electronic surveillance of telephone and e-mail telecommunications into and out of the United States.

The various United States government defendants in these cases (collectively, "the United States") have moved to dismiss and/or seeks summary judgment as to all claims in both cases, summarizing their arguments in nearly identical fashion thusly: "the Court lacks subject matter jurisdiction with respect to plaintiffs' statutory claims against the United States because Congress has not waived sovereign immunity, and summary judgment for the Government on all of plaintiffs' remaining claims against all parties (including any claims not dismissed for lack of jurisdiction) is required because information necessary to litigate plaintiffs' claims is properly subject to and excluded from use in the case by the state secrets privilege and related statutory privileges." Jewel, C 08-4373 Doc #18 at 2; see also Shubert, C 07-0693 Doc #680/38[1] at 2.

For the reasons stated herein, the court has determined that neither group of plaintiffs/purported class representatives has alleged an injury that is sufficiently particular to those plaintiffs or to a distinct group to which those plaintiffs belong; rather, the harm alleged is a generalized grievance shared in

[1] Citations to documents in the Shubert docket will be in the following format: Doc #xxx/yy, with the first number corresponding to the MDL docket (M:06-1791) and the second corresponding to the individual docket (C:07-0693).

substantially equal measure by all or a large class of citizens. "[I]njuries that are shared and generalized —— such as the right to have the government act in accordance with the law —— are not sufficient to support standing." Seegers v Gonzales, 396 F3d 1248, 1253 (DC Cir 2005).

Accordingly, these actions must be, and hereby are, DISMISSED with prejudice. The various other grounds advanced by the Unites States are not ruled on herein and form no part of the basis for this order. Judgment shall be entered against plaintiffs in both actions.

I

A

In December 2005, news agencies began reporting that President George W Bush had ordered the NSA to conduct, without warrants, eavesdropping of some portion of telecommunications in the United States and that the NSA had obtained the cooperation of telecommunications companies to tap into a significant portion of the companies' telephone and e-mail traffic, both domestic and international. See, e g, James Risen and Eric Lichtblau, Bush Lets US Spy on Callers Without Courts, NY Times (Dec 16, 2005). A copy of this article is attached.

In January 2006, the first of dozens of lawsuits by customers of telecommunications companies were filed alleging various causes of action related to such cooperation with the NSA in warrantless wiretapping of customers' communications. One such lawsuit was Hepting v AT&T Corp, C 06-0672 VRW (ND Cal filed January 31, 2006). The four plaintiffs in that suit were Tash

Hepting, Gregory Hicks, Erik Knutzen and Carolyn Jewel. In addition to the dozens of cases filed against telecommunications companies, several were filed against United States government entities by individuals claiming to have been surveilled. In six states, officials with oversight authority over public utilities initiated administrative proceedings to investigate telecommunications companies' alleged assistance to the NSA.

Several of the cases arising from the NSA's alleged warrantless electronic surveillance were originally venued in the Northern District of California; others were filed in federal district courts throughout the United States. The instant case brought by plaintiff Virginia Shubert and her co-plaintiffs against George W Bush and other government officials was filed May 17, 2006 in the Eastern District of New York.

In 2006, the United States filed lawsuits seeking to enjoin state officials in Maine, New Jersey, Connecticut, Vermont and Missouri from pursuing their investigations into the alleged disclosure of customer telephone records by various telecommunication carriers to the NSA. These motions were based, in general, on the Supremacy Clause of the United States Constitution, the foreign affairs power of the federal government and the state secrets privilege (SSP).

In the Hepting case and the other cases in which individual plaintiffs sought to sue telecommunications companies, the United States moved to intervene and simultaneously to dismiss, asserting the SSP and arguing, in essence, that the SSP required immediate dismissal because no further progress in the litigation was possible without compromising national security. C 06-0672 VRW

Doc ##122-125. The telecommunications company defendants in the case also moved to dismiss on other grounds. C 06-0672 VRW Doc #86.

On July 20, 2006 the court denied the motions to dismiss, holding that: the SSP did not categorically bar plaintiffs' action; the subject matter of the action was not a state secret; the SSP would not prevent the telecommunications company defendants from disclosing whether they had received certifications authorizing the alleged assistance to the government; statutory privileges did not bar the action; plaintiff customers had sufficiently alleged injury-in-fact to establish standing; and neither a purported common law immunity nor the doctrine of qualified immunity prevented plaintiffs from proceeding against the telecommunications company defendants. The court certified its order for an interlocutory appeal pursuant to 28 USC § 1292(b), but denied the United States' request for a stay of proceedings pending appeal. Hepting v AT&T Corp, 439 F Supp 2d 974 (ND Cal 2006).

On August 9, 2006, the Judicial Panel on Multidistrict Litigation ordered all cases arising from the alleged warrantless wiretapping program by the NSA transferred to the Northern District of California and consolidated before the undersigned judge.

On July 24, 2007, the court denied the United States' motion for summary judgment in its actions to enjoin the state officials' investigations. The court determined that the states' investigations into wiretapping activities did not violate the doctrine of intergovernmental immunity, were not preempted by federal statutes and did not infringe on the federal government's power over foreign affairs to a constitutionally impermissible

degree. M 06-1791 Doc #334; 2007 WL 2127345. Because the Hepting appeal was then pending, the court refrained from considering the government's assertion of the SSP.

On August 30, 2007, the court heard a number of motions including the United States' motion to dismiss the Shubert case (Doc #295/yy). Doc #368.

On March 14, 2008, the Ninth Circuit entered an order withdrawing the submission in the Hepting case. CA Docket No 06-17132, Doc #109. In light of that order, this court terminated the pending motion to dismiss in Shubert shortly afterward giving the United States leave to petition the court to re-open the motion at the next case management conference in the matter should the circumstances so warrant. Doc #438.

On July 10, 2008, Congress amended the Foreign Intelligence Surveillance Act of 1978 ("FISA"), 50 USC §§1801-71, by enacting the FISA Amendments Act of 2008, Pub L No 110-261, 122 Stat 2436 (FISAAA), codified at 50 USC §1885a. Of special relevance to these cases, the new law included a provision for the benefit of telecommunications companies that allowed the United States to invoke a newly-created immunity and thus seek dismissal of cases brought against telecommunications companies by certifying that certain narrowly-defined circumstances were present, including, as relevant to this litigation, that the defendant had "provided assistance to an element of the intelligence community * * * in connection with an intelligence activity involving communications that was —— (I) authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007; and (ii) designed to detect or prevent a terrorist

attack, or activities in preparation for a terrorist attack, against the United States." FISAAA also contained a provision (section 803) depriving states of authority to: investigate; require through regulation or any other means the disclosure of information about; impose any administrative sanction for; or commence or maintain a civil action pertaining to "alleged assistance to an element of the intelligence community" into an electronic communication service provider. 50 USC §1885b.

On August 28, 2008, the Ninth Circuit remanded Hepting v AT&T without rendering a decision "in light of the FISA Amendments Act of 2008." CA Docket No 06-17137 (9th Cir) Doc #116.

On September 18, 2008, plaintiffs Carolyn Jewel, Tash Hepting, Gregory Hicks, Erik Knutzen and Joice Walton —— all, with the exception of Walton, named plaintiffs in the Hepting action —— filed the instant lawsuit against the NSA and various government officials. Pursuant to Rule of Procedure of the Judicial Panel on Multidistrict Litigation 7.5(a), Jewel was reassigned to the undersigned judge but not added to the MDL docket.

On September 19, 2008, the United States filed its motion to dismiss all claims against telecommunications company defendants in these cases, including the pending master consolidated complaints based on section 802 of FISAAA. Doc #469. On December 23, 2008, the United States moved for summary judgment in the "state cases" relying on section 803 of FISAAA. Doc #536. On June 3, 2009, the court granted both motions, finding the provisions of FISAAA at issue on the motions constitutional and therefore enforceable by the United States in the manner prescribed by statute. Doc ##639, 640.

The June 3 orders left only five MDL cases —— those brought by private individuals and entities and naming United States government officials and agencies as defendants (Al-Haramain Islamic Foundation, Inc et al v Bush et al, No C 07-0109; Center for Constitutional Rights et al v Bush e al, No C 07-1115; Guzzi v Bush, No C 06-6225; Shubert et al v Bush et al, No C 07-0693) and one "tagalong action" transferred by order of the MDL Panel after the United States' motions were filed (McMurray et al v Verizon Communications Inc et al, C 09-0131) —— and Jewel v NSA. The motions by the United States and the telecommunications company defendants to dismiss the McMurray case were argued on June 3 and, after reviewing supplemental briefs, the court dismissed McMurray. Doc #661.

This concludes the general procedural history; a discussion of the specific motions that are the subjects of this order now follows.

B

Jewel v NSA. In Jewel, meanwhile, the United States "government defendants" in their official capacities filed the instant motion (on April 3, 2009) asking the court to "dismiss plaintiffs' statutory claims for lack of jurisdiction, uphold the Government's privilege assertions, enter summary judgment for the Government Defendants, and dismiss the case as to all defendants and all claims." C 08-4373 Doc #18 at 35. Plaintiffs filed an opposition (Doc #29), and defendants replied (Doc #31).

Those defendants sued in their individual capacities —— George W Bush, Richard B Cheney, David S Addington, Keith B

Alexander, Michael V Hayden, John D McConnell, John D Negroponte, Michael B Mukasey, Alberto R Gonzales, and John D Ashcroft (see Doc #14) —— (some of whom had become private citizens in the intervening months) sought to avoid responding to the complaint pending the outcome of the dispositive motion and moved the court for an order relieving them of the responsibility to respond (Doc #32), a step which prompted plaintiffs to file a counter-motion for "relief from improper motion for reconsideration by individual capacity defendants." Doc #33. The court heard arguments on the dispositive motion on July 15, 2009, after which plaintiffs requested —— and obtained —— leave to file a supplemental brief on the scope of FISA preemption of the SSP (Doc ##38, 40); the United States responded with its own supplemental brief on September 4, 2009. Doc #46. On September 17, 2009, the court held a hearing on the individual capacity defendants' request to defer responding to the complaint and the plaintiffs' counter-motion. Doc #47.

The fifty-five-page complaint contains seventeen causes of action. It alleges that plaintiffs are, variously, "an individual residing in Livermore, California [who] has been a subscriber and user of AT&T's residential long distance telephone service since February 1995; an individual residing in San Jose, California [who] has been a subscriber and user of AT&T's residential long distance telephone service since February 1995; an individual residing in Petaluma, California [who] has been a subscriber and user of AT&T's WorldNet dial-up internet service since approximately June 2000; an individual residing in Los Angeles, California [who] has been a subscriber and user of AT&T's

WorldNet dial-up internet service from at least October 2003 until May 2005; and an individual residing in San Jose, California [who] is a current subscriber and user of AT&T's WorldNet dial-up internet service. Doc #1 at 5, ¶¶20-24.

The complaint alleges a factual narrative beginning with President George W Bush's approval of, and the NSA's and various government officials' implementation of, surveillance activities inside the United States without statutory authorization or court approval, including electronic surveillance of Americans' telephone and internet communications (id ¶¶39-49); these allegations have in some form appeared in a number of books and thousands of print and broadcast media stories and blog posts and, accordingly, can now fairly be characterized as common knowledge to most Americans. The Jewel complaint also contains allegations about AT&T's involvement in the surveillance activities that are quite similar to those set forth in the complaint in Hepting and discussed in the court's opinion in that case, to wit, that AT&T and the NSA maintained special rooms at a Folsom Street facility in San Francisco for purposes of carrying out surveillance of AT&T's communications networks. ¶¶50-81. 439 F Supp 2d at 989-90. Plaintiffs also allege that since October 2001, defendants have "continually solicited and obtained the disclosure" of all information in AT&T's major databases of stored telephone and Internet records and that these records include the records of plaintiffs' phone and/or internet use. ¶¶82-97. The complaint contains no other allegations specifically linking any of the plaintiffs to the alleged surveillance activities.

\\

The complaint purports to set forth seventeen causes of action against the United States and defendant government officials in their official and individual capacities, claiming that the alleged actions violate the First and Fourth Amendments of the United States Constitution and the separation of powers doctrine, as well as various statutory provisions —— section 109 of FISA, 50 USC §1809; the Wiretap Act, as amended by the Electronic Communications Privacy Act, 18 USC §2511(1)(a), (1)(c), (1)(d) and(3)(a); and the Stored Communications Act, 18 USC §2703(a), (b) and (c). Because the defendants are sued in both their official and individual capacities, the originally-named defendants remain in the suit in their individual capacities only, while new holders of their offices are substituted in as defendants for official-capacity purposes pursuant to FRCP 25(d).[2]

Plaintiffs seek declaratory, injunctive and other equitable relief, including: a declaration that the surveillance program as alleged violates plaintiffs' rights under the First and Fourth Amendments, 18 USC §2511, 18 USC §2703, 50 USC §1809, the Administrative Procedure Act and the constitutional separation-of-powers principle; an injunction prohibiting defendants' continued use of the program and requiring the defendants to turn over an inventory of their pertinent stored communications and records; statutory, actual and punitive damages to the extent permitted by law and according to proof; and attorney fees. Doc #1 at 53.

---

[2] Rule 25(d) provides: "An action does not abate when a public officer who is a party in an official capacity dies, resigns, or otherwise ceases to hold office while the action is pending. The officer's successor is automatically substituted as a party."

B

Shubert v Bush. The parties held a telephonic status conference on September 3, 2009 in which the United States announced its intention to renew its motion to dismiss. The court offered the parties the opportunity to supplement their earlier submissions on the motion and set a briefing schedule. After a series of stipulated continuances assertedly due to a Department of Justice re-evaluation of the circumstances in which the United States would invoke the SSP in litigation (Doc ##674, 679), the United States filed its motion on October 30. The matter was fully briefed and the court heard arguments and took the matter under submission on December 15, 2009.

The Shubert complaint, which has never been amended, alleges that each of the plaintiffs resides and works in Brooklyn, New York and, variously: "frequently calls and sends emails to the United Kingdom, France and Italy and has made similar communications as part of her work"; "frequently calls and sends emails to family and friends in Egypt from her home, and has made telephone calls as a part of her work"; "regularly makes phone calls and sends email both within the United States [and] calls the Netherlands and sends emails to the Netherlands and Norway from her home"; "makes phone calls and sends email both within the United States, and outside the United States." As to each plaintiff, the complaint alleges "a good faith basis to believe that she, like so many millions of Americans, has been surveilled without a warrant pursuant to the illegal Spying Program." Doc #1 at 3, ¶¶ 5-8. Defendants named in the complaint are current and former government officials George W Bush, Michael V Hayden, Keith B Alexander,

Alberto Gonzales, John Ashcroft and Does 1-100. The current holders of the various offices held by the originally-named defendants have been substituted pursuant to FRCP 25(d).

Plaintiffs' factual allegations rely on the above-referenced December 2005 New York Times article, on public statements by the President and on other publicly available information (Complaint ¶ 46-92). The complaint contains no factual allegations specifically linking any of the plaintiffs to the alleged surveillance activities; it contains only the allegations of domestic and international telephone and electronic mail use. The complaint alleges only interception of plaintiffs' communications, but not, as in the other cases in this MDL and in Jewel, collection and storage of records of monitored communications.

The complaint purports to set forth causes of action under: FISA's section 1810 asserting that they, as "aggrieved persons]" are entitled to damages under 50 USC § 1810; the ECPA; the SCA; and the Fourth Amendment. Plaintiffs seek certification of their suit as a class action; a declaratory judgment on all claims; an award of liquidated and/or compensatory damages; an award of punitive damages; and attorney fees and costs.

II

Upon careful consideration of the allegations of both complaints, the court has concluded that neither the Jewel plaintiffs nor the Shubert plaintiffs have alleged facts sufficient to establish their standing to proceed with their lawsuit against

\\

the President, the NSA and the other high-level government officials named as defendants in these lawsuits.

Although most of the plaintiffs and nearly all of the relevant factual allegations are the same as in Hepting, the standing problem presented in these cases is markedly different. In Hepting, the court rejected the AT&T defendants' arguments for dismissal based on lack of standing, noting that plaintiffs' status as customers of AT&T who used its telecommunications services was sufficient to withstand the motion to dismiss for lack of standing:

> AT & T also contends ''[p]laintiffs lack standing to assert their statutory claims (Counts II–VII) because the FAC alleges no facts suggesting that their statutory rights have been violated'' and ''the FAC alleges nothing to suggest that the named plaintiffs were themselves subject to surveillance.'' * * * But AT & T ignores that the gravamen of plaintiffs' complaint is that AT & T has created a dragnet that collects the content and records of its customers' communications. See, e g, FAC, ¶¶ 42–64. The court cannot see how any one plaintiff will have failed to demonstrate injury-in-fact if that plaintiff effectively demonstrates that all class members have so suffered. * * * As long as the named plaintiffs were, as they allege, AT & T customers during the relevant time period (FAC, ¶¶ 13–16), the alleged dragnet would have imparted a concrete injury on each of them.

439 F Supp 2d at 1000. Citing FEC v Akins, 524 US 11 (1998), the court also rejected AT&T's contention that the diffuse nature of the harm from the alleged dragnet deprived individual AT&T customers of standing:

> This conclusion is not altered simply because the alleged injury is widely shared among AT & T customers.
>
> * * *
>
> Here, the alleged injury is concrete even though it is widely shared. Despite AT&T's alleged creation of a dragnet to intercept all or substantially all of its

> customers' communications, this dragnet necessarily inflicts a concrete injury that affects each customer in a distinct way, depending on the content of that customer's communications and the time that customer spends using AT&T services. Indeed, the present situation resembles a scenario in which "large numbers of individuals suffer the same common-law injury (say, a widespread mass tort."

439 F Supp 2d at 1001.

Whereas the gravamen of the Hepting plaintiffs' complaint was rooted in a contractual relationship between private parties, the Jewel and Shubert cases, boiled to their essence, are both efforts by citizens seeking to redress alleged misfeasance by the executive branch of the United States government.

As the court noted in Hepting, "[w]hether styled as a constitutional or prudential limit on standing, the [Supreme] Court has sometimes determined that where large numbers of Americans suffer alike, the political process, rather than the judicial process, may provide the more appropriate remedy for a widely shared grievance." Id at 1000, quoting FEC v Akins, 524 US 11, 23. This special species of standing problem is directly relevant here.

Stated more generally, "[s]tanding will be denied to one alleging only a generalized interest, shared by a large segment of the public. * * * The courts do not want to be viewed as a panacea of all of society's ills, a task too large and often inappropriate for them to handle. If an injury is far-reaching, it is likely that a better solution would come from a political forum." Charles H Koch, Jr, 33 Federal Practice and Procedure: Judicial Review of Administrative Action § 8413 at 452.

A considerable jurisprudence has developed around United States citizens and taxpayers attempting to challenge government

actions or the manner in which Congress or the executive branch manages and spends public funds. By and large, these challenges have failed on standing grounds:

> Because the interests of the taxpayer are, in essence, the interests of the public at large, deciding a constitutional claim based solely on taxpayer standing "would be, not to decide a judicial controversy, but to assume a position of authority over the governmental acts of another and co-equal department, an authority which plainly we do not possess."

Hein v Freedom From Religion Foundation, 551 US 587, 601 (2007), quoting Frothingham v Mellon, 262 US 447, 489 (1923).

Cases in which plaintiffs sue the government in order to stop or expose constitutional or other transgressions by government officials present special standing considerations. A citizen may not gain standing by claiming a right to have the government follow the law. Ex parte Levitt, 302 US 633 (1937). The essence of standing is the party's direct, personal stake in the outcome as opposed to the issues the party seeks to have adjudicated in the litigation:

> The fundamental aspect of standing is that it focuses on the party seeking to get his complaint before a federal court and not on the issues he wishes to have adjudicated. The "gist of the question of standing" is whether the party seeking relief has "alleged such a personal stake in the outcome of the controversy as to assure that concrete adverseness which sharpens the presentation of issues upon which the court so largely depends for illumination of difficult constitutional questions."

Flast v Cohen, 392 US 83, 99 (1968), quoting Baker v Carr, 369 US 186, 204 (1962).

The two cases at bar are, in essence, citizen suits seeking to employ judicial remedies to punish and bring to heel high-level government officials for the allegedly illegal and

unconstitutional warrantless electronic surveillance program or programs now widely, if incompletely, aired in the public forum. Plaintiffs have attempted to present their complaint as something narrower than a generalized grievance by alleging interference with their telephone and/or broadband internet subscription and/or use. But such allegations do not avoid the problem. Telephone subscribership and internet use are widespread on the scale of the paying of taxes or the holding of United States citizenship: in November 2005, 92.9% of United States households subscribed to telephone service —— 107 million households in all.[3] In December 2005, there were 51,218,145 high-speed internet connections in the United States; one year later, there were 82,809,845; by the end of 2007, there were over 100,000,000.[4] Allegations of telephone use for international calls do not fare much better.

These cases allege both statutory and constitutional violations. This court has written at length in another case in this MDL, Al-Haramain Islamic Foundation, Inc v Bush et al, about the allegations necessary to make out a prima facie case to establish "aggrieved person" status in a lawsuit based on electronic surveillance (see, for example, 50 USC §1801(k)). 564 F Supp 2d 1109(ND Cal 2008); 595 F Supp 2d 1077 (ND Cal 2009). In

---

[3] Alexander Belinfante, Telephone Subscribership In The United States (Data through November 2006), Industry Analysis and Technology Division Wireline Competition Bureau, Federal Communications Commission (May 2007)at 6, Table 1 http://www.fcc.gov/Document_Indexes/WCB/2007_index_WCB_Report.html, DOC-272904A1.pdf (consulted December 29, 2009).

[4] "High-Speed Services for Internet Access: Status as of June 30, 2007," Industry Analysis and Technology Division, Wireline Competition Bureau, Federal Communications Commission (March 2008)at 7, Table 1. Available at http://www.fcc.gov/Document_Indexes/WCB/2008_index_WCB_Report.html, DOC-280906A1.pdf (consulted December 29, 2009).

that case, plaintiffs were able to allege in an amended complaint following dismissal of their original complaint "a sequence of events pertaining directly to the government's investigations of Al-Haramain Oregon" and the court denied the government's motion to dismiss the amended complaint. 595 F Supp 2d at 1079. While plaintiffs in Jewel and Shubert assert that they are aggrieved, they neither allege facts nor proffer evidence sufficient to establish a prima facie case that would differentiate them from the mass of telephone and internet users in the United States and thus make their injury "concrete and particularized" consonant with the principles articulated in Lujan v Defenders of Wildlife, 504 US 555, 560 (1992).

As for plaintiffs' constitutional claims, "when a court is asked to undertake constitutional adjudication, the most important and delicate of its responsibilities, the requirement of concrete injury further serves the function of insuring that such adjudication does not take place unnecessarily." Schlesinger v Reservists Committee to Stop the War, 418 US 208, 221 (1974). This is especially true when, as here, the constitutional issues at stake in the litigation seek judicial involvement in the affairs of the executive branch and national security concerns appear to undergird the challenged actions. In such cases, only plaintiffs with strong and persuasive claims to Article III standing may proceed.

III

Because the court GRANTS the United States' motions to dismiss based on the specific standing grounds stated herein, the

court declines to rule on the sovereign immunity, SSP and other issues raised in the United States' motions.

For the reasons stated herein, the government defendants' motion to dismiss in Jewel el al v NSA et al, C 08-4373 Doc #18, is GRANTED. Inasmuch as plaintiffs lack the particularized injury to afford them standing to sue defendants in their official capacities, so also plaintiffs lack standing to pursue claims against defendants as individuals. The substitution of new individuals into certain official positions during the pendency of these actions does not affect this conclusion and hence renders moot the motions at docket numbers 32 and 33 pertaining to the obligation of the defendants sued in their individual capacity to respond to the complaint. The motions at docket numbers 32 and 33 are therefore DENIED. Further, the court's ruling renders moot plaintiffs' substitution of John C Yoo and Jack L Goldsmith for Doe defendants 1 and 2, respectively. Doc #56. Plaintiffs therefore are DENIED leave to amend the complaint.

For the reasons stated herein, the United States' motion to dismiss in Shubert et al v Obama et al, C 07-0693 Doc #38 (MDL Doc #680) is GRANTED.

The clerk is directed to close these two files and to terminate all pending motions.

IT IS SO ORDERED.

VAUGHN R WALKER
United States District Chief Judge

12/16/05 N.Y. Times A1
2005 WLNR 20281359

New York Times (NY)

December 16, 2005

Section: A

Bush Lets U.S. Spy on Callers Without Courts

JAMES RISEN and ERIC LICHTBLAU; Barclay Walsh contributed research for this article.

National Security Agency officials privately voice concern about legality of eavesdropping on Americans and others inside United States without court-approved warrants, as secretly authorized by Pres Bush in wake of 9/11 attacks; at issue is NSA's monitoring of international telephone calls and e-mail messages inside US in search of evidence of terrorist activity under presidential order signed in 2002; dozen current and former agency officials question whether this surveillance has stretched, if not crossed, constitutional limits on legal searches; Bush administration views operation as necessary so agency can move quickly on threats to US; defenders of program say it has been critical tool in helping disrupt terrorist plots and prevent attacks inside US; critics say most people targeted for NSA monitoring have never been charged with crime; it is not clear how much members of Congress were told about presidential order and eavesdropping program; photo; timeline of NSA's half-century of surveillance (L)

WASHINGTON, Dec. 15 Months after the Sept. 11 attacks, President Bush 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, according to government officials.

Under a presidential order signed in 2002, the intelligence agency has monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people inside the United States without warrants over the past three years in an effort to track possible "dirty numbers" linked to Al Qaeda, the officials said. The agency, they said, still seeks warrants to monitor entirely domestic communications.

The previously undisclosed decision to permit some eavesdropping inside the country without court approval was a major shift in American intelligence-gathering practices, particularly for the National Security Agency, whose mission is to spy on communications abroad. As a result, some officials familiar with the continuing operation have questioned whether the surveillance has stretched, if not crossed, constitutional limits on legal searches.

"This is really a sea change," said a former senior official who specializes in national security law. "It's almost a mainstay of this country that the N.S.A. only does foreign searches."

Nearly a dozen current and former officials, who were granted anonymity because of the classified nature of the program, discussed it with reporters for The New York Times because of their concerns about the operation's legality and oversight.

According to those officials and others, reservations about aspects of the program have also been expressed by Senator John D. Rockefeller IV, the West Virginia Democrat who is the vice chairman of the Senate Intelligence Committee, and a judge presiding over a secret court that oversees intelligence matters. Some of the questions about the agency's new powers led the administration to temporarily suspend the operation last year and impose more restrictions, the officials said.

The Bush administration views the operation as necessary so that the agency can move quickly to monitor communications that may disclose threats to the United States, the officials said. Defenders of the program say it has been a critical tool in helping disrupt terrorist plots and prevent attacks inside the United States.

Administration officials are confident that existing safeguards are sufficient to protect the privacy and civil liberties of Americans, the officials say. In some cases, they said, the Justice Department eventually seeks warrants if it wants to expand the eavesdropping to include communications confined within the United States. The officials said the administration had briefed Congressional leaders about the program and notified the judge in charge of the Foreign Intelligence Surveillance Court, the secret Washington court that deals with national security issues.

The White House asked The New York Times not to publish this article, arguing that it could jeopardize continuing investigations and alert would-be terrorists that they might be under scrutiny. After meeting with senior administration officials to hear their concerns, the newspaper delayed publication for a year to conduct additional reporting. Some information that administration officials argued could be useful to terrorists has been omitted.

Dealing With a New Threat

While many details about the program remain secret, officials familiar with it say the N.S.A. eavesdrops without warrants on up to 500 people in the United States at any given time. The list changes as some names are added and others dropped, so the number monitored in this country may have reached into the thousands since the program began, several officials said. Overseas, about 5,000 to 7,000 people suspected of terrorist ties are monitored at one time, according to those officials.

Several officials said the eavesdropping program had helped uncover a plot by Iyman Faris, an Ohio trucker and naturalized citizen who pleaded guilty in 2003 to supporting Al Qaeda by planning to bring down the Brooklyn Bridge with blowtorches. What appeared to be another Qaeda plot, involving fertilizer bomb attacks on British pubs and train stations, was exposed last year in part through the program, the officials said. But they said most people targeted for N.S.A. monitoring have never been charged with a crime, including an Iranian-American doctor in the South who came under suspicion because of what one official described as dubious ties to Osama bin Laden.

The eavesdropping program grew out of concerns after the Sept. 11 attacks that the nation's intelligence agencies were not poised to deal effectively with the new threat of Al Qaeda and that they were handcuffed by legal and bureaucratic restrictions better suited to peacetime than war, according to officials. In response, President Bush significantly eased limits on American intelligence and law enforcement agencies and the military.

But some of the administration's antiterrorism initiatives have provoked an outcry from members of Congress, watchdog groups, immigrants and others who argue that the measures erode protections for civil liberties and intrude on Americans' privacy.

Opponents have challenged provisions of the USA Patriot Act, the focus of contentious debate on Capitol Hill this week, that expand domestic surveillance by giving the Federal Bureau of Investigation more power to collect information like library lending lists or Internet use. Military and F.B.I. officials have drawn criticism for monitoring what were largely peaceful antiwar protests. The Pentagon and the Department of Homeland Security were forced to retreat on plans to use public and private databases to hunt for possible terrorists. And last year, the Supreme Court rejected the administration's claim that those labeled "enemy combatants" were not entitled to judicial review of their open-ended detention.

Mr. Bush's executive order allowing some warrantless eavesdropping on those inside the United States -- including American citizens, permanent legal residents, tourists and other foreigners -- is based on classified legal opinions that assert that the president has broad powers to order such searches, derived in part from the September 2001 Congressional resolution authorizing him to wage war on Al Qaeda and other terrorist groups, according to the officials familiar with the N.S.A. operation.

The National Security Agency, which is based at Fort Meade, Md., is the nation's largest and most secretive intelligence agency, so intent on remaining out of public view that it has long been nicknamed "No Such Agency." It breaks codes and maintains listening posts around the world to eavesdrop on foreign governments, diplomats and trade negotiators as well as drug lords and terrorists. But the agency ordinarily operates under tight restrictions on any spying on Americans, even if they are overseas, or disseminating information about them.

What the agency calls a "special collection program" began soon after the Sept. 11 attacks, as it looked for new tools to attack terrorism. The program accelerated in early 2002 after the Central Intelligence Agency started capturing top Qaeda operatives overseas, including Abu Zubaydah, who was arrested in Pakistan in March 2002. The C.I.A. seized the terrorists' computers, cellphones and personal phone directories, said the officials familiar with the program. The N.S.A. surveillance was intended to exploit those numbers and addresses as quickly as possible, they said.

In addition to eavesdropping on those numbers and reading e-mail messages to and from the Qaeda figures, the N.S.A. began monitoring others linked to them, creating an expanding chain. While most of the numbers and addresses were overseas, hundreds were in the United States, the officials said.

Under the agency's longstanding rules, the N.S.A. can target for interception phone calls or e-mail messages on foreign soil, even if the recipients of those communications are in the United States. Usually, though, the government can only target phones and e-mail messages in the United States by first obtaining a court order from the Foreign Intelligence Surveillance Court, which holds its closed sessions at the Justice Department.

Traditionally, the F.B.I., not the N.S.A., seeks such warrants and conducts most domestic eavesdropping. Until the new program began, the N.S.A. typically limited its domestic surveillance to foreign embassies and missions in Washington, New York and other cities, and obtained court orders to do so.

Since 2002, the agency has been conducting some warrantless eavesdropping on people in the United States who are linked, even if indirectly, to suspected terrorists through the chain of phone numbers and e-mail addresses, according to several officials who know of the operation. Under the special program, the agency monitors their international communications, the officials said. The agency, for example, can target phone calls from someone in New York to someone in Afghanistan.

Warrants are still required for eavesdropping on entirely domestic-to-domestic communications, those officials say, meaning that calls from that New Yorker to someone in California could not be monitored without first going to the Federal Intelligence Surveillance Court.

A White House Briefing

After the special program started, Congressional leaders from both political parties were brought to Vice President Dick Cheney's office in the White House. The leaders, who included the chairmen and ranking members of the Senate and House intelligence committees, learned of the N.S.A. operation from Mr. Cheney, Lt. Gen. Michael V. Hayden of the Air Force, who was then the agency's director and is now a full general and the principal deputy

director of national intelligence, and George J. Tenet, then the director of the C.I.A., officials said.

It is not clear how much the members of Congress were told about the presidential order and the eavesdropping program. Some of them declined to comment about the matter, while others did not return phone calls.

Later briefings were held for members of Congress as they assumed leadership roles on the intelligence committees, officials familiar with the program said. After a 2003 briefing, Senator Rockefeller, the West Virginia Democrat who became vice chairman of the Senate Intelligence Committee that year, wrote a letter to Mr. Cheney expressing concerns about the program, officials knowledgeable about the letter said. It could not be determined if he received a reply. Mr. Rockefeller declined to comment. Aside from the Congressional leaders, only a small group of people, including several cabinet members and officials at the N.S.A., the C.I.A. and the Justice Department, know of the program.

Some officials familiar with it say they consider warrantless eavesdropping inside the United States to be unlawful and possibly unconstitutional, amounting to an improper search. One government official involved in the operation said he privately complained to a Congressional official about his doubts about the program's legality. But nothing came of his inquiry. "People just looked the other way because they didn't want to know what was going on," he said.

A senior government official recalled that he was taken aback when he first learned of the operation. "My first reaction was, 'We're doing what?' " he said. While he said he eventually felt that adequate safeguards were put in place, he added that questions about the program's legitimacy were understandable.

Some of those who object to the operation argue that is unnecessary. By getting warrants through the foreign intelligence court, the N.S.A. and F.B.I. could eavesdrop on people inside the United States who might be tied to terrorist groups without skirting longstanding rules, they say.

The standard of proof required to obtain a warrant from the Foreign Intelligence Surveillance Court is generally considered lower than that required for a criminal warrant -- intelligence officials only have to show probable cause that someone may be "an agent of a foreign power," which includes international terrorist groups -- and the secret court has turned down only a small number of requests over the years. In 2004, according to the Justice Department, 1,754 warrants were approved. And the Foreign Intelligence Surveillance Court can grant emergency approval for wiretaps within hours, officials say.

Administration officials counter that they sometimes need to move more urgently, the officials said. Those involved in the program also said that the N.S.A.'s eavesdroppers might need to start monitoring large batches of numbers all at once, and that it would be impractical to seek permission from the Foreign Intelligence Surveillance Court first, according to the officials.

The N.S.A. domestic spying operation has stirred such controversy among some national security officials in part because of the agency's cautious culture and longstanding rules.

Widespread abuses -- including eavesdropping on Vietnam War protesters and civil rights activists -- by American intelligence agencies became public in the 1970's and led to passage of the Foreign Intelligence Surveillance Act, which imposed strict limits on intelligence gathering on American soil. Among other things, the law required search warrants, approved by the secret F.I.S.A. court, for wiretaps in national security cases. The agency, deeply scarred by the scandals, adopted additional rules that all but ended domestic spying on its part.

After the Sept. 11 attacks, though, the United States intelligence community was criticized for being too risk-averse. The National Security Agency was even cited by the independent 9/11 Commission for adhering to self-imposed rules that were stricter than those set by federal law.

Concerns and Revisions

Several senior government officials say that when the special operation began, there were few controls on it and little formal oversight outside the N.S.A. The agency can choose its eavesdropping targets and does not have to seek approval from Justice Department or other Bush administration officials. Some agency officials wanted nothing to do with the program, apparently fearful of participating in an illegal operation, a former senior Bush administration official said. Before the 2004 election, the official said, some N.S.A. personnel worried that the program might come under scrutiny by Congressional or criminal investigators if Senator John Kerry, the Democratic nominee, was elected president.

In mid-2004, concerns about the program expressed by national security officials, government lawyers and a judge prompted the Bush administration to suspend elements of the program and revamp it.

For the first time, the Justice Department audited the N.S.A. program, several officials said. And to provide more guidance, the Justice Department and the agency expanded and refined a checklist to follow in deciding whether probable cause existed to start monitoring someone's communications, several officials said.

A complaint from Judge Colleen Kollar-Kotelly, the federal judge who oversees the Federal Intelligence Surveillance Court, helped spur the suspension, officials said. The judge questioned whether information obtained under the N.S.A. program was being improperly used as

the basis for F.I.S.A. wiretap warrant requests from the Justice Department, according to senior government officials. While not knowing all the details of the exchange, several government lawyers said there appeared to be concerns that the Justice Department, by trying to shield the existence of the N.S.A. program, was in danger of misleading the court about the origins of the information cited to justify the warrants.

One official familiar with the episode said the judge insisted to Justice Department lawyers at one point that any material gathered under the special N.S.A. program not be used in seeking wiretap warrants from her court. Judge Kollar-Kotelly did not return calls for comment.

A related issue arose in a case in which the F.B.I. was monitoring the communications of a terrorist suspect under a F.I.S.A.-approved warrant, even though the National Security Agency was already conducting warrantless eavesdropping.

According to officials, F.B.I. surveillance of Mr. Faris, the Brooklyn Bridge plotter, was dropped for a short time because of technical problems. At the time, senior Justice Department officials worried what would happen if the N.S.A. picked up information that needed to be presented in court. The government would then either have to disclose the N.S.A. program or mislead a criminal court about how it had gotten the information.

Several national security officials say the powers granted the N.S.A. by President Bush go far beyond the expanded counterterrorism powers granted by Congress under the USA Patriot Act, which is up for renewal. The House on Wednesday approved a plan to reauthorize crucial parts of the law. But final passage has been delayed under the threat of a Senate filibuster because of concerns from both parties over possible intrusions on Americans' civil liberties and privacy.

Under the act, law enforcement and intelligence officials are still required to seek a F.I.S.A. warrant every time they want to eavesdrop within the United States. A recent agreement reached by Republican leaders and the Bush administration would modify the standard for F.B.I. wiretap warrants, requiring, for instance, a description of a specific target. Critics say the bar would remain too low to prevent abuses.

Bush administration officials argue that the civil liberties concerns are unfounded, and they say pointedly that the Patriot Act has not freed the N.S.A. to target Americans. "Nothing could be further from the truth," wrote John Yoo, a former official in the Justice Department's Office of Legal Counsel, and his co-author in a Wall Street Journal opinion article in December 2003. Mr. Yoo worked on a classified legal opinion on the N.S.A.'s domestic eavesdropping program.

At an April hearing on the Patriot Act renewal, Senator Barbara A. Mikulski, Democrat of

Maryland, asked Attorney General Alberto R. Gonzales and Robert S. Mueller III, the director of the F.B.I., "Can the National Security Agency, the great electronic snooper, spy on the American people?"

"Generally," Mr. Mueller said, "I would say generally, they are not allowed to spy or to gather information on American citizens."

President Bush did not ask Congress to include provisions for the N.S.A. domestic surveillance program as part of the Patriot Act and has not sought any other laws to authorize the operation. Bush administration lawyers argued that such new laws were unnecessary, because they believed that the Congressional resolution on the campaign against terrorism provided ample authorization, officials said.

The Legal Line Shifts

Seeking Congressional approval was also viewed as politically risky because the proposal would be certain to face intense opposition on civil liberties grounds. The administration also feared that by publicly disclosing the existence of the operation, its usefulness in tracking terrorists would end, officials said.

The legal opinions that support the N.S.A. operation remain classified, but they appear to have followed private discussions among senior administration lawyers and other officials about the need to pursue aggressive strategies that once may have been seen as crossing a legal line, according to senior officials who participated in the discussions.

For example, just days after the Sept. 11, 2001, attacks on New York and the Pentagon, Mr. Yoo, the Justice Department lawyer, wrote an internal memorandum that argued that the government might use "electronic surveillance techniques and equipment that are more powerful and sophisticated than those available to law enforcement agencies in order to intercept telephonic communications and observe the movement of persons but without obtaining warrants for such uses."

Mr. Yoo noted that while such actions could raise constitutional issues, in the face of devastating terrorist attacks "the government may be justified in taking measures which in less troubled conditions could be seen as infringements of individual liberties."

The next year, Justice Department lawyers disclosed their thinking on the issue of warrantless wiretaps in national security cases in a little-noticed brief in an unrelated court case. In that 2002 brief, the government said that "the Constitution vests in the President inherent authority to conduct warrantless intelligence surveillance (electronic or otherwise) of foreign powers or their agents, and Congress cannot by statute extinguish that constitutional authority."

Administration officials were also encouraged by a November 2002 appeals court decision in an unrelated matter. The decision by the Foreign Intelligence Surveillance Court of Review, which sided with the administration in dismantling a bureaucratic "wall" limiting cooperation between prosecutors and intelligence officers, cited "the president's inherent constitutional authority to conduct warrantless foreign intelligence surveillance."

But the same court suggested that national security interests should not be grounds "to jettison the Fourth Amendment requirements" protecting the rights of Americans against undue searches. The dividing line, the court acknowledged, "is a very difficult one to administer."

Photo: In 2002, President Bush toured the National Security Agency at Fort Meade, Md., with Lt. Gen. Michael V. Hayden, who was then the agency's director and is now a full general and the principal deputy director of national intelligence. (Photo by Doug Mills/Associated Press)(pg. A16)

Chart: "A Half-Century of Surveillance"

HISTORY -- Created in 1952, the National Security Agency is the biggest American intelligence agency, with more than 30,000 employees at Fort Meade, Md., and listening posts around the world. Part of the Defense Department, it is the successor to the State Department's "Black Chamber" and American military eavesdropping and code-breaking operations that date to the early days of telegraph and telephone communications.

MISSION -- The N.S.A. runs the eavesdropping hardware of the American intelligence system, operating a huge network of satellites and listening devices around the world. Traditionally, its mission has been to gather intelligence overseas on foreign enemies by breaking codes and tapping into telephone and computer communications.

SUCCESSES -- Most of the agency's successes remain secret, but a few have been revealed. The agency listened to Soviet pilots and ground controllers during the shooting down of a civilian South Korean airliner in 1983; traced a disco bombing in Berlin in 1986 to Libya through diplomatic messages; and, more recently, used the identifying chips in cellphones to track terrorist suspects after the 2001 attacks.

DOMESTIC ACTIVITY -- The disclosure in the 1970's of widespread surveillance on political dissenters and other civil rights abuses led to restrictions at the N.S.A. and elsewhere on the use of domestic wiretaps. The N.S.A. monitors United Nations delegations and some foreign embassy lines on American soil, but is generally prohibited from listening in on the conversations of anyone inside the country without a special court order.

OFFICIAL RULES -- Since the reforms of the late 1970's, the N.S.A. has generally been permitted to target the communications of people on American soil only if they are believed to be "agents of a foreign power" -- a foreign nation or international terrorist group -- and a warrant is obtained from the Foreign Intelligence Surveillance Court.

EXPANDED ROLE -- Months after the terror attacks of Sept. 11, 2001, President Bush

signed a secret executive order that relaxed restrictions on domestic spying by the N.S.A., according to officials with knowledge of the order. The order allows the agency to monitor without warrants the international phone calls and e-mail messages of some Americans and others inside the United States.

(pg. A16)

December 28, 2005, Wednesday - Because of an editing error, a front-page article on Dec. 16 about a decision by President Bush to authorize the National Security Agency to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without warrants ordinarily required for domestic spying misstated the name of the court that would normally issue those warrants. It is the Foreign -- not Federal --Intelligence Surveillance Court.

---- INDEX REFERENCES ---

COMPANY: JUSTICE DEPARTMENT; PENTAGON LTD; STATE DEPARTMENT; CENTRAL INTELLIGENCE AGENCY; DEFENSE DEPARTMENT; UNITED NATIONS

NEWS SUBJECT: (Legal (1LE33); Social Issues (1SO05); Judicial (1JU36); International Terrorism (1IN37); Legislation (1LE97); United Nations (1UN54); Government (1GO80); Crime (1CR87); Civil Rights Law (1CI34); World Organizations (1IN77); Criminal Law (1CR79); Economics & Trade (1EC26); Political Parties (1PO73); Sept 11th Aftermath (1SE05); Public Affairs (1PU31))

INDUSTRY: (Smuggling & Illegal Trade (1SM35); Aerospace & Defense (1AE96); Defense (1DE43); Security (1SE29); Defense Intelligence (1DE90); Homeland Security (1HO11); Aerospace & Defense Regulatory (1AE25))

REGION: (North America (1NO39); Americas (1AM92); USA (1US73))

Language: EN

OTHER INDEXING: (Risen, James; Lichtblau, Eric; Bush, George W (Pres)) (AIR FORCE; BROOKLYN BRIDGE; CENTRAL INTELLIGENCE AGENCY; CONGRESS; CONSTITUTION; DEFENSE DEPARTMENT; DEMOCRATIC; DEPARTMENT OF HOMELAND; FEDERAL INTELLIGENCE SURVEILLANCE COURT; FEDERAL BUREAU OF INVESTIGATION; FOREIGN INTELLIGENCE SURVEILLANCE ACT; FOREIGN INTELLIGENCE SURVEILLANCE COURT; FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW; HOUSE; HOUSE ON; JUSTICE DEPARTMENT; LEGAL LINE SHIFTS; NATIONAL SECURITY AGENCY; NSA; OSAMA; PATRIOT ACT; PENTAGON; SENATE; SENATE INTELLIGENCE COMMITTEE; STATE DEPARTMENT; SUPREME COURT; US SPY; UNITED NATIONS; USA; USA PATRIOT ACT; WHITE HOUSE) (Abu Zubaydah; Al Qaeda; Alberto R. Gonzales; Barbara A. Mikulski; Bush; Cheney; Colleen Kollar-Kotelly; Dick Cheney; Doug Mills; Faris; Generally; George J. Tenet; Iyman Faris; John D. Rockefeller; John Kerry; John Yoo; Judge Kollar; Kotelly; Mi-

chael V. Hayden; Months; Mueller; Pres Bush; Qaeda; Revisions; Robert S. Mueller; Rockefeller; Traditionally; Yoo) (Terrorism; Surveillance of Citizens by Government; Wiretapping and Other Eavesdropping Devices and Methods; Electronic Mail; Freedom and Human Rights; Terrorism; Terrorism)

EDITION: Late Edition - Final

Word Count: 4957
12/16/05 NYT A1
END OF DOCUMENT