

~~SECRET~~

## FOREIGN INTELLIGENCE SURVEILLANCE COURT

IN RE DIRECTIVES TO YAHOO!, INC  
PURSUANT TO SECTION 105B OF THE  
FOREIGN INTELLIGENCE  
SURVEILLANCE ACT

Dkt. No. 105B(G) 07-01

Yahoo! Inc.'s Memorandum in  
Opposition to Motion to Compel

UNDER SEAL

MARC J. ZWILLINGER  
Sonnenschein Nath & Rosenthal LLP  
1301 K Street, N.W.  
Suite 600; East Tower  
Washington, DC 20005  
Tel: (202) 408-6400  
Fax: (202) 408-6399  
mzwillinger@sonnenschein.com

*Attorney for Yahoo! Inc.*

November 30, 2007

~~SECRET~~

Classified by: Derivatively classified from material classified by Margaret  
A. Skelly-Nolan, Acting Counsel for Intelligence Policy,  
NSD, DOJ

Reason: 1.4(c)

Declassify on 21 November 2032

~~SECRET~~

## TABLE OF CONTENTS

Table of Contents .....	i
Table of Authorities .....	ii
Request for Hearing and Statement Concerning Classified Information .....	v
Introduction .....	1
Factual Background .....	2
A. Yahoo! .....	2
B. FISA and the Protect America Act .....	2
C. The Directives .....	5
Argument .....	6
A. Standard of Review .....	6
B. The Directives Violate the Fourth Amendment .....	6
1. The Fourth Amendment Applies To the Acquisition of the Communications of U.S. Citizens That is Authorized By The Directives .....	7
a) U.S. Citizens Abroad .....	7
b) U.S. Citizens in the United States .....	9
2. The Directives Violate The Fourth Amendment By Authorizing Warrantless Surveillance .....	10
a) The Fourth Amendment Prohibits Warrantless Surveillance .....	11
3. There are No Applicable Warrant Exceptions In This Case .....	13
a) The Supreme Court has Not Recognized a Foreign Intelligence Exception To The Warrant Requirement to Obtain Communications of U.S. citizens .....	13
b) The PAA is Inconsistent with Any Lower Court Decision Recognizing a Foreign Intelligence Exception .....	15
c) No Other Exceptions To The Warrant Requirement Apply .....	17
4. The Directives Require Unreasonable Searches .....	19
C. The PAA Violates the Separation of Powers and is Otherwise Flawed .....	21
D. The Directives Improperly Implement the PAA .....	24
Conclusion .....	25
Certificate of Service .....	26

~~SECRET~~

## TABLE OF AUTHORITIES

Cases:

<i>Bell v. Wolfish</i> , 441 U.S. 520 (1979).....	18
<i>Berger v. State of New York</i> , 388 U.S. 41 (1967) .....	11, 12, 13, 22
<i>Camara v. Municipal Court</i> , 387 U.S. 523 (1967) .....	22
<i>City of Indianapolis v. Edmond</i> , 531 U.S. 32 (2000) .....	18
<i>Coolidge v. New Hampshire</i> , 403 U.S. 443 (1971) .....	11
<i>Delaware v. Prouse</i> , 440 U.S. 648 (1979) .....	22
<i>Doe v. Gonzales</i> , 500 F. Supp. 2d 379 (S.D.N.Y. 2007).....	21, 22, 23
<i>Georgia v. Randolph</i> , 547 U.S. 103 (2006) .....	10
<i>Katz v. United States</i> , 389 U.S. 347 (1967).....	<i>passim</i>
<i>Marbury v. Madison</i> , 5 U.S. 137 (1803) .....	23
<i>Mayfield v. United States</i> , 504 F. Supp. 2d 1023 (D. Or. 2007) .....	18, 19
<i>Mincey v. Arizona</i> , 437 U.S. 385 (1978).....	22
<i>Rakas v. Illinois</i> , 439 U.S. 128 (1978) .....	9
<i>Reid v. Covert</i> , 354 U.S. 1 (1957) .....	8
<i>In re Sealed Case</i> , 310 F.3d 717 (FISCR 2002).....	<i>passim</i>
<i>Stonehill v. United States</i> , 405 F.2d 738 (9th Cir. 1968) .....	8
<i>Terry v. Ohio</i> , 392 U.S. 1 (1968) .....	18
<i>Trulock v. Freeh</i> , 275 F.3d 391, 403 (4 <sup>th</sup> Cir. 2001) .....	7
<i>United States v. Behety</i> , 32 F.3d 503 (11th Cir. 1994).....	8
<i>United States v. Biasucci</i> , 786 F.2d 504 (2d Cir. 1986) .....	19
<i>United States v. Brignoni-Ponce</i> , 422 U.S. 873 (1975) .....	18
<i>United States v. Buckner</i> , 473 F.3d 551 (4th Cir. 2007) .....	7

~~SECRET~~

<i>United States v. Butenko</i> , 494 F.2d 593 (3d Cir. 1974).....	16, 17, 18
<i>United States v. Cavanagh</i> , 807 F.2d 787 (9th Cir. 1987) .....	2, 3
<i>United States v. Conroy</i> , 589 F.2d 1258 (5th Cir. 1979).....	8
<i>United States v. Falls</i> , 34 F.3d 674 (8th Cir. 1994) .....	19
<i>United States v. Duggan</i> , 743 F.2d 59 (2d Cir. 1984).....	3
<i>United States v. Heckenkamp</i> , 482 F.3d 1142 (9th Cir. 2007).....	7
<i>United States v. Johnson</i> , 952 F.2d 565 (1st Cir. 1991).....	3
<i>United States v. Karo</i> , 458 U.S. 705 (1984).....	9, 10
<i>United States v. Martinez-Fuerte</i> , 428 U.S. 543 (1976) .....	18
<i>United States v. Mesa-Rincon</i> , 911 F.2d 1433 (10th Cir. 1990) .....	19
<i>United States v. Mount</i> , 757 F.2d 1315 (D.C. Cir. 1985).....	8
<i>United States v. Pelton</i> , 835 F.2d 1067 (4th Cir. 1987) .....	3
<i>United States v. Truong Dinh Hung</i> , 629 F.2d 908 (4th Cir. 1980).....	16, 17, 18, 19
<i>United States v. United States District Court ("Keith")</i> , 407 U.S. 297 (1972).....	<i>passim</i>
<i>United States v. Verdugo-Urquidez</i> , 494 U.S. 259 (1990).....	8
<i>Vernonia School District 47 J v. Acton</i> , 515 U.S. 646 (1995) .....	18
<i>Zweibon v. Mitchell</i> , 516 F.2d 594 (D.C. Cir. 1975) .....	14, 15

Statutes:

18 U.S.C. § 2709 .....	22
------------------------	----

## Foreign Intelligence Surveillance Act of 1978

50 U.S.C. § 1801 .....	3, 4, 6
50 U.S.C. § 1802 .....	3
50 U.S.C. § 1804 .....	3

- iii -

~~SECRET~~

~~SECRET~~

50 U.S.C. § 1805 ..... 3, 4, 5

Protect America Act of 2007

50 U.S.C. § 1805a ..... *passim*

50 U.S.C. § 1805b ..... *passim*

50 U.S.C. § 1805c ..... *passim*

Other:

U.S. Const. Amend. IV ..... 11

~~SECRET~~

~~SECRET~~**REQUEST FOR HEARING**

Yahoo! respectfully requests a hearing and seeks to appear at such hearing, through counsel, in the Washington, D.C. area.

**STATEMENT CONCERNING CLASSIFIED INFORMATION**

Yahoo! and undersigned counsel have been provided access to classified information.

- v -

~~SECRET~~

~~SECRET~~

## INTRODUCTION

Yahoo! Inc. ("Yahoo!"), a leading provider of internet communications services, opposes the United States' Motion to Compel Compliance with Directives of the Director of National Intelligence and Attorney General ("Mot. to Compel"), which seeks to compel Yahoo! to comply with [REDACTED] Directives issued to it ("the Directives") pursuant to Section 105B(e) of the Protect America Act of 2007 ("PAA"). These Directives purport to require Yahoo! to capture and disclose the private communications of an unknown and unlimited number of yet-to-be identified users.

Yahoo! has not complied with the Directives because of concerns that the Directives require Yahoo! to assist in conducting warrantless surveillance that is likely to capture private communications of United States citizens located in the U.S. and abroad. The Supreme Court has never sanctioned warrantless surveillance of U.S. citizens. Because warrantless invasions of the privacy of U.S. citizens run counter to the core principles of the Fourth Amendment, Yahoo! wanted the opportunity to raise the Constitutional issues before this court. Based on Supreme Court jurisprudence, and the precedent of the Foreign Intelligence Surveillance Court of Review ("FISCR"),<sup>1</sup> the surveillance of U.S. citizens permitted by the PAA does not satisfy the Fourth Amendment. Accordingly, the Directives—as well as the recent 2007 amendments to the Foreign Intelligence Surveillance Act ("FISA") by the Protect America Act ("PAA") —are unconstitutional to the extent they authorize the surveillance of U.S. citizens with no prior judicial review.

Moreover, the limitations on judicial review contained in the PAA violate the separation of powers. The PAA improperly constrains the ability of the judiciary to fulfill its constitutional mandate to ensure the constitutionality of the laws passed by the legislative branch and the actions taken by the executive branch. Accordingly, the provisions of the PAA that seek to dictate to this Court the appropriate level of judicial review render the PAA unconstitutional.

---

<sup>1</sup> *In re Sealed Case*, 310 F.3d 717 (FISCR 2002)..

~~SECRET~~

~~SECRET~~

Finally, even if the PAA is constitutional, the Directives appear to bypass the few provisions of the PAA that provide limitations on the government surveillance activity. Specifically, the PAA requires that the government file a certification that the contemplated acquisition "does not constitute electronic surveillance." Unlike the required certification that "there are reasonable procedures in place for determining that the acquisition of information under this section concerns persons reasonably believed to be located outside the U.S.," a certification that the acquisition does not constitute electronic surveillance cannot be made now for yet-to-be-identified persons. By allowing the government to "identify from time to time" the users whose communications must be intercepted and disclosed, the Directives are inconsistent with the PAA's certification requirements with respect to persons not yet identified by the government.

Consequently, Yahoo! requests that the government's Motion to Compel be denied.

#### FACTUAL BACKGROUND

##### A. Yahoo!

Yahoo! is a leading global internet communications, commerce, and media company that offers a comprehensive network of services to more than 500 million individuals each month. Using Yahoo!'s services, users can log on to their password-protected accounts from anywhere in the world and communicate with anyone anywhere in the world, including by sending emails through Yahoo! Mail, exchanging real-time written communications through Yahoo! instant messaging ("IM"), and by using the computer like a telephone by using the Voice over IP ("VOIP") features of Yahoo! Messenger. Users can also store emails, documents, photos and other files in their accounts.

##### B. FISA and the Protect America Act

Prior to the 2007 Amendments to FISA passed as part of the PAA, the FISA statute had been reviewed and declared to be consistent with the Fourth Amendment to the Constitution by



~~SECRET~~

several courts, including the Foreign Intelligence Surveillance Court of Review ("FISCR"). *See, e.g., United States v. Duggan*, 743 F.2d 59, 74 (2d Cir. 1984); *United States v. Cavanagh*, 807 F.2d 787, 789-90 (9th Cir. 1987); *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987); *United States v. Johnson*, 952 F.2d 565, 573 (1st Cir. 1991); *In re Sealed Case*, 310 F.3d at 746. These courts had generally approved of FISA's procedures, which enable federal officers, authorized by the Attorney General, to obtain orders from this Court to conduct "electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information." 50 U.S.C. § 1802(b).<sup>2</sup>

In order to obtain a FISA Order, the applying officer must state the "facts and circumstances relied upon by the applicant to justify his belief that--the target of the electronic surveillance is a foreign power or an agent of a foreign power," 50 U.S.C. § 1804(a)(4), and an executive official must, among other things, certify that a significant purpose<sup>3</sup> of the surveillance is to obtain foreign intelligence information that cannot reasonably be obtained using normal investigative techniques. 50 U.S.C. § 1804(a)(7). That application is reviewed by this Court to determine, among other things, whether probable cause exists to believe that the target is a foreign power or its agent. 50 U.S.C. § 1805(a)(3). If the target is a U.S. person, the Court engages in an additional level of judicial review regarding the nature and purpose of the surveillance. 50 U.S.C. § 1805(a)(5).

Despite the careful balance that FISA reflected, on August 4, 2007, Congress passed the PAA, which provides the executive branch with substantial new authority to acquire the private communications of persons, including U.S. citizens, who are reasonably believed to be located

<sup>2</sup> The terms "foreign power," "agent of a foreign power" and "foreign intelligence information," are all defined terms meant to ensure that the targets subject to surveillance and the information sought by that surveillance are generally related to either foreign governments, political organizations, entities or terrorists. 50 U.S.C. § 1801(a),(b),(e).

<sup>3</sup> The phrase "a significant purpose" replaced "the purpose" due to the amendments made to FISA by the USA PATRIOT ACT. The FISA Court of Review ("FISCR") found this change to be constitutional, principally because all of the procedural protections of FISA remained in place. *See* 310 F.3d at 746.

~~SECRET~~

~~SECRET~~

overseas, whether or not such individuals have engaged in wrongdoing or are agents of a foreign power. The PAA does this, in part, by excluding from FISA's definition of "electronic surveillance" surveillance directed at persons reasonably believed to be outside the U.S. Instead of the prior judicial review provided by FISA, the PAA allows the DNI and the AG to direct providers to intercept and disclose communications of their users after certifying to the FISA court, that:

(1) there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States, and such procedures will be subject to review of the Court pursuant to section 1805c of this title; (2) the acquisition does not constitute electronic surveillance<sup>4</sup>; (3) the acquisition involves obtaining the foreign intelligence information from or with the assistance of a communications service provider, custodian, or other person . . . who has access to communications, either as they are transmitted or while they are stored . . . ; (4) a significant purpose of the acquisition is to obtain foreign intelligence information; and (5) the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section 1801(h) of this title.

50 U.S.C. § 1805b(a).

Under the PAA, the certification is "not required to identify the specific facilities, places, premises, or property at which the acquisition of foreign intelligence information will be directed."

50 U.S.C. § 1805b(b). Once a certification is made, the government can issue a directive to any provider requiring it to "immediately provide the Government with all information, facilities, and assistance necessary to accomplish the acquisition." 50 U.S.C. § 1805b(e).

Absent from the PAA is any prior judicial review of a directive by a detached and neutral magistrate. Absent is any judicial review of the purpose of the intelligence gathering. Absent is any probable cause showing by the government that the target of the surveillance is an agent of a

<sup>4</sup> "Electronic surveillance" is defined in FISA, and generally includes the acquisition by "electronic, mechanical, or other surveillance device" of wire or radio communications. 50 U.S.C. § 1801(f). The PAA specifically states that "[n]othing in the definition of electronic surveillance under section 1801(f) of this title shall be construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States." Nevertheless, acquisitions to be performed under a directive constitute "surveillance" as that term is commonly understood. See 50 U.S.C. § 1805a.

~~SECRET~~

~~SECRET~~

foreign power. Absent is any additional level of review when the target is known to be a U.S. citizen. Instead, the only form of judicial review is a review of the procedures by which the government determines that any acquisitions conducted pursuant to Section 105B "do not constitute electronic surveillance." 50 U.S.C. § 1805c(a). This review is restricted to the sole question of whether the government's determination is clearly erroneous. 50 U.S.C. § 1805c(b).

C. The Directives

On [REDACTED], undersigned counsel for Yahoo! was served with [REDACTED] directives pursuant to the PAA.<sup>5</sup> The operative language of the Directives is identical and provides that:

The government will [REDACTED]

[REDACTED] Yahoo Inc. . . is hereby directed, pursuant to section 105B(c)(1) of the Act, to immediately provide the Government with all information, facilities, and assistance necessary to accomplish this acquisition with a minimum of interference with the services that Yahoo provides.<sup>6</sup>

Over the course of several months, Yahoo! attended many meetings with representatives of the government during which Yahoo! explained its appreciation of the important national security interests at stake, but also its concerns regarding the constitutionality of the PAA as well as its misgivings about the government's planned implementation of the then-anticipated Directives. On [REDACTED], immediately after being served with the Directives, Yahoo! sent a detailed letter to the Department of Justice, reiterating Yahoo!'s concerns and articulating its interest in briefing the issues before this Court if the government continued to seek to pursue the acquisition contemplated

<sup>5</sup> Copies of the Directives are attached as Exhibit 1 to the Government's Motion to Compel.

<sup>6</sup> Mot. to Compel, Ex. 1 at 2.

~~SECRET~~

~~SECRET~~

by the Directives. On November 21, 2007, the government filed a motion pursuant to Section 105B(g) of FISA to compel Yahoo! to comply with the Directives. That motion was served on Yahoo!'s counsel on November 28, 2007.

## ARGUMENT

### A. Standard of Review

Pursuant to Section 105B(g) of FISA, the government may invoke the aid of this Court to compel compliance with a Directive issued pursuant to Section 105B(e). This Court "shall issue an order requiring the person [to whom the directive is issued] to comply with the directive if it finds the directive was issued in accordance with subsection (e) and is otherwise lawful." 50 U.S.C. § 1805b(g). Accordingly, this Court may only compel Yahoo!'s compliance if it finds that the Directives are procedurally proper and do not violate statutory or constitutional law.

### B. The Directives Violate the Fourth Amendment

The Directives, and the PAA from which they originate, violate the Fourth Amendment to the United States Constitution for the reasons set forth in detail in the sections below. First, because the Directives encompass interceptions of private communications of U.S. citizens at home and abroad, the Fourth Amendment is implicated.<sup>7</sup> Second, the Fourth Amendment requires prior judicial authorization through a search warrant, or a warrant equivalent. Third, no previously recognized exceptions to the warrant requirement apply because the Supreme Court has never recognized a foreign intelligence interception to the warrant requirement. Fourth, even if the Court would recognize such an exemption, it would not do so under the circumstances presented by the PAA. Finally, the procedures of the PAA are not sufficiently close to the wiretap procedures set out in Title III of the Omnibus Crime and Safe Streets Act ("Title III") to be considered "reasonable" under Fourth Amendment jurisprudence.

---

<sup>7</sup> Yahoo! does not dispute that the Fourth Amendment does not apply to non-U.S. persons located outside the United States (Mot. to Compel at 6).

~~SECRET~~

1. *The Fourth Amendment Applies To the Acquisition of the Communications of U.S. Citizens Authorized By the Directives*

The Directives require Yahoo! to capture and disclose the private communications of U.S. citizens, *i.e.*, surveillance that is clearly subject to the requirements of the Fourth Amendment even though directed at persons "reasonably believed to be located outside of the United States" 50 U.S.C. § 1805a. The Directives encompass surveillance of U.S. citizens in two ways: (a) surveillance that targets U.S. citizens who are temporarily abroad; and (b) surveillance that captures communications of U.S. citizens at home who are communicating with the target of the surveillance.<sup>8</sup> Under those two situations, the surveillance authorized by the Directive invades the reasonable expectation of privacy of U.S. citizens and must, therefore, comply with the Fourth Amendment. *See Katz v. United States*, 389 U.S. 347, 352 (1967) (telephone surveillance must comply with Fourth Amendment); *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007) (reasonable expectation of privacy in personal computer); *Trulock v. Freeh*, 275 F.3d 391, 403 (4<sup>th</sup> Cir. 2001) (reasonable expectation of privacy in password protected electronic files).

a) U.S. Citizens Abroad

The Directives require Yahoo! to assist in the surveillance of U.S. citizens who are abroad, even temporarily, because the Directives cover communications of anyone so long as they are "reasonably believed to be located outside of the United States." 50 U.S.C. § 1805a. Thus, a U.S. citizen traveling or living overseas can be the intended target of a directive.

In this scenario, the Fourth Amendment applies with full force, despite the fact that the targeted citizen is outside of the U.S. The Supreme Court has not had occasion to address the issue of the extraterritorial application of the Fourth Amendment to U.S. citizens, but the Court has generally held that the "Bill of Rights . . . should not be stripped away just because [a United States

<sup>8</sup> The "minimization" procedures required by the PAA are not guaranteed to result in the suppression of communications of U.S. citizens because the government may nevertheless retain those communications despite the minimization requirements. *See* 50 U.S.C. § 1801(h).

~~SECRET~~

citizen] happens to be in another land.” *Reid v. Covert*, 354 U.S. 1, 6 (1957). That holding is particularly germane to the Fourth Amendment which the Court has held “protects people, not places.” *Katz*, 389 U.S. at 351. Moreover, in *United States v. Verdugo-Urquidez*, cited in the government’s motion to compel, the Court recognized that “the purpose of the Fourth Amendment was to protect *the people of the United States* against arbitrary action by their own Government.” *United States v. Verdugo-Urquidez*, 494 U.S. 259, 266 (1990).<sup>9</sup> Accordingly, Supreme Court precedent strongly suggests that the Fourth Amendment applies to U.S. citizens abroad.

The courts that have addressed this issue have reached the same conclusion. The Fifth Circuit has held that “[t]he Fourth Amendment not only protects all within our bounds; it also shelters our citizens wherever they may be in the world from unreasonable searches by our own government.” *United States v. Conroy*, 589 F.2d 1258, 1264 (5th Cir. 1979). Similarly, other circuits have implicitly acknowledged this principle by endorsing the so called “joint venture doctrine,” which holds that a search of a U.S. citizen by foreign agents may violate the Fourth Amendment—and be subject to the exclusionary rule—if conducted in close association with U.S. agents. *See, e.g., United States v. Behety*, 32 F.3d 503, 510 (11th Cir. 1994) (noting that Fourth Amendment applies to search of U.S. citizen when U.S. law enforcement substantially participates in the search or if the foreign officials are acting as agents for their U.S. counterparts.); *United States v. Mount*, 757 F.2d 1315, 1318 (D.C. Cir. 1985) (same); *Stonehill v. United States*, 405 F.2d 738, 743 (9th Cir. 1968) (“the Fourth Amendment could apply to raids by foreign officials only if Federal agents so substantially participated in the raids so as to convert them into joint ventures between the U.S. and the foreign officials”).

Moreover, the surveillance authorized by the PAA extends beyond extra-territorial surveillance of U.S. citizens. Because the Directives cover surveillance for up to one year when

---

<sup>9</sup> In *Verdugo-Urquidez*, the Court held there was no Fourth Amendment violation when U.S. officers searched the Mexican residence of a Mexican citizen who had no voluntary ties to the U.S.

~~SECRET~~



~~SECRET~~

directed at a person reasonably believed to be located outside of the United States, 50 U.S.C. § 1805b(a), it is possible that the "target" may return to the U.S. during the surveillance period. Therefore, the Directives may target U.S. citizens who may be in the U.S. when under surveillance.

b) U.S. Citizens in the United States.

The Directives also cover the communications of U.S. citizens in the U.S. so long as those communications are with individuals who are "reasonably believed to be located outside of the United States." 50 U.S.C. § 1805a. Thus, the Directives will cause Yahoo! to capture the communications of a U.S. citizen sitting in his bedroom in Kansas while communicating in real-time to someone located overseas, who may also be a U.S. citizen temporarily located abroad.

The Fourth Amendment undisputedly applies to electronic surveillance of U.S. citizens located in the U.S. *See Katz*, 389 U.S. at 352. The fact that such citizens are not the "targets" of the surveillance does not diminish the applicability of Fourth Amendment protections. To the contrary, in *Rakas v. Illinois*, the Supreme Court explicitly rejected the "so-called 'target' theory" of Fourth Amendment analysis. *Rakas v. Illinois*, 439 U.S. 128, 133 (1978). Instead, the Court stated that whether a person can claim the protection of the Fourth Amendment depends not on whether they are the target of a particular search, but "upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy." *Id.* at 143. Here, U.S. citizens, sitting in their homes and communicating in real-time by voice [REDACTED] or email have a reasonable expectation of privacy against warrantless surveillance against them by their own government.

The fact that the surveillance of a U.S. citizen's communications is "directed at" a person on the other end of the communication who may be outside the reach of the Fourth Amendment does not eliminate the Fourth Amendment protection for the U.S. citizen. That citizen's reasonable expectation of privacy is not diminished simply because he is speaking to someone who might be subject to government monitoring. In *United States v. Karo*, the Supreme Court found the planting of an electronic tracking device without a warrant violated the Fourth Amendment. *United States v.*

~~SECRET~~

~~SECRET~~

*Karo*, 468 U.S. 705 (1984). In reaching that conclusion, the plurality opinion authored by Justice White rejected the argument that simply because a tracking device might have been carried in by a guest, the government's planting of such a device would not infringe a reasonable expectation of privacy. *Id.* at 716 n.4. Justice White found it unreasonable to assume that individuals undertake the risk that an acquaintance has "been bugged by the Government without his knowledge or consent." *Id.* Such an argument, he observed, would undercut the central holding of *Katz* because it could then be argued that "Katz had no reasonable expectation of privacy in his conversation because the person to whom he was speaking might have divulged the contents of the conversation." *Id.* Here too, the fact that the person with whom a United States citizen is communicating may be the unwitting target of government surveillance does not diminish the Fourth Amendment privacy rights of the incidentally affected United States citizen. *See also Georgia v. Randolph*, 547 U.S. 103, 105 (2006) (wife's consent to search house did not eliminate the need to evaluate husband's Fourth Amendment rights to be free from unwarranted search).

The conclusion that the Fourth Amendment rights of the U.S. citizen are not diminished when they are communicating with someone overseas is particularly warranted here, where -- unlike an obviously foreign telephone number -- [REDACTED] do not generally signal the geographic location of the user. Consequently, U.S. citizens whose communications are captured by the Directives may have no way of knowing that they are communicating with persons located outside the U.S.

2. *The Directives Violate the Fourth Amendment by Authorizing Warrantless Surveillance*

To the extent that the Directives, and the PAA under which they are issued, permit the surveillance of U.S. citizens' communications with no prior judicial authorization, such warrantless surveillance is inconsistent with U.S. citizens' Fourth Amendment rights. The Fourth Amendment to the United States Constitution provides that:

~~SECRET~~



~~SECRET~~

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. Amend. IV.

The surveillance to be performed under the Directives is not being conducted pursuant to a warrant.<sup>10</sup> As set forth below, under black letter constitutional law, "searches conducted outside the judicial process, without prior approval by a magistrate, are per se unreasonable under the Fourth Amendment -- subject only to a few specifically established and well-delineated exceptions." *Katz*, 389 U.S. at 357. Therefore, the surveillance of U.S. citizens under the PAA's authority cannot be justified unless it falls within an exception to the warrant requirement, or unless, under the jurisprudence of the FISC, the procedures for the issuance of a Directive so closely approximate the warrant process that they are deemed reasonable. *In re Sealed Case*, 310 F.3d at 746.

a) The Fourth Amendment Prohibits Warrantless Surveillance

Recognizing that "[f]ew threats to liberty exist which are greater than that posed by the use of eavesdropping devices," *Berger v. State of New York*, 388 U.S. 41, 63 (1967), the Supreme Court has never authorized the warrantless electronic surveillance of U.S. citizens. Instead, the Court has repeatedly recognized that such surveillance is constitutionally impermissible when the officers of the government have not been required "to present their estimate of probable cause for detached scrutiny by a neutral magistrate." *Katz*, 389 U.S. at 356.

In *Katz v. United States*, the Court reaffirmed the need for a warrant before conducting electronic surveillance. The Court held that warrantless electronic surveillance of a call made from

<sup>10</sup> The certification clearly does not constitute a warrant, in that, among other things, it is not issued by a magistrate or judge. *Coolidge v. New Hampshire*, 403 U.S. 443, 449 (1971) (warrant invalid if not issued by a "neutral and detached" magistrate). Moreover, the certification does not "identify the specific facilities, places, premises, or property at which the acquisition of foreign intelligence information will be directed." 50 U.S.C. § 1805b(b). The Fourth Amendment, by contrast, requires that a warrant "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. Amend. IV.

~~SECRET~~

a public telephone booth violated the Fourth Amendment. The Court placed particular emphasis on the lack of a warrant, holding that even if the officers "did no more here than they might properly have done with prior judicial sanction," there was nevertheless a constitutional violation because "searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject to only a few specifically established and well-delineated exceptions." *Katz*, 389 U.S. at 356-57.

But the involvement of a neutral magistrate alone is not sufficient to address Fourth Amendment concerns. In *Berger v. New York*, the Court struck down a New York statute that provided for judicial authorization of broad electronic surveillance based on nothing more than the submission to the court of a sworn statement by a law enforcement officer that "there is reasonable ground to believe that evidence of crime may be thus obtained." *Berger*, 388 U.S. at 54. The court held that such "broadside authorization" of electronic surveillance, even by a detached and neutral authority, was not the equivalent to a warrant as it was not carefully circumscribed but permitted general searches by electronic devices. *Id.* at 58. Without a warrant that met the probable cause and the particularity requirements of the Fourth Amendment, the Court concluded that the statute violated the "command of the Fourth Amendment," and was therefore unconstitutional. *Id.* at 63.

In short, *Berger* and *Katz*, the Supreme Court's two seminal cases on the warrant requirement of the Fourth Amendment, are directly on point here. They both make clear that U.S. citizens may not be subject to surveillance unless a warrant based on probable cause is first obtained from a neutral magistrate. Furthermore, under the particularity requirements of the Fourth Amendment, the authority to conduct such surveillance must be carefully circumscribed, and not permit the government excessive discretion. Here, the Directives served pursuant to the PAA are neither issued by a detached and neutral magistrate nor contain the required particularity to survive Fourth Amendment scrutiny. Instead, they represent the type of blanket authorization that the court

~~SECRET~~

rejected in *Berger*. Accordingly, the PAA, and the Directives are unconstitutional to the extent they cover surveillance of U.S. citizens.<sup>11</sup>

### 3. *There are No Applicable Warrant Exceptions in This Case*

The Supreme Court has never recognized a general exception to the Fourth Amendment's warrant requirement for electronic surveillance of U.S. citizens, whether for criminal investigations, domestic security, or foreign intelligence purposes. *See Katz*, 389 U.S. at 357; *United States v. United States District Court ("Keith")*, 407 U.S. 297 (1972).

- a) The Supreme Court has Not Recognized a Foreign Intelligence Exception to the Warrant Requirement to Obtain Communications of U.S. Citizens

When presented with the opportunity to consider whether to find a domestic security exception to the warrant requirement in the *Keith* case, the Supreme Court declined to do so, holding that warrantless government surveillance of U.S. citizens was unconstitutional even when undertaken for the legitimate purposes of national security. *Id.* at 320. In *Keith*, the government had conducted electronic surveillance of an individual charged with bombing a CIA building based on the Attorney General's belief that the surveillance was "necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government." *Id.* at 300. In deciding whether to create an exception to the prior judicial scrutiny requirement for surveillance for national security purposes, the Court balanced "the duty of Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression." *Id.* at 314-15. The Court acknowledged the legitimacy of the security concerns at issues and accepted that the surveillance may have been the kind that "readily would have gained prior judicial approval." *Id.* at 317. Nevertheless, the Court concluded that the Fourth

<sup>11</sup> Even to the extent such communications are minimized, that does not prevent a constitutional violation. The Supreme Court in *Katz* specifically held that the absence of a warrant rendered the surveillance unconstitutional, even though "the surveillance was limited, both in scope and duration, . . . and they took great care to overhear only the conversations of the petitioner himself." *Katz*, 389 U.S. at 354.

~~SECRET~~

~~SECRET~~

Amendment did not allow—even for national security reasons—an exception to the warrant requirement for electronic surveillance given “the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillance to oversee political dissent.” *Id.* at 320.

Although the Court did not address whether an exception could exist for surveilling U.S. citizens for *foreign* national security concerns, its holding is equally applicable in that context. Like intelligence gathering for domestic security purposes, intelligence gathering for foreign purposes: (a) may involve special circumstances necessary to protect national security, (b) may not be an “attempt to gather specific evidence of criminal prosecutions,” (c) may raise issues with which courts are not particularly experienced, and (d) may require great secrecy. Yet, these arguments were raised by the government in *Keith*, and the Court nevertheless found that even such weighty concerns could not justify entrusting the essential freedoms of U.S. citizens to the sole discretion of the executive branch:

The Fourth Amendment does not contemplate the executive officer of Government as neutral and disinterested magistrates. . . . The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressure to obtain incriminating evidence and overlook potential invasions of privacy and protected speech . . . . The Fourth Amendment contemplates a prior judicial judgment, not the risk that executive discretion may be reasonably exercised.

*Id.* at 317. That fundamental principal is not changed by the fact that the current threat to national security is both foreign and domestic. The D.C. Circuit, in a plurality opinion in *Zweibon v. Mitchell*, 516 F.2d 594 (D.C. Cir. 1975), reached the same conclusion. *Zweibon* concluded that none of the *Keith* factors--such as judicial competence, secrecy and expediency--were sufficient to justify creating an exception to the warrant requirement. *Id.* at 641-51. In particular, the *Zweibon* opinion found that even though the executive branch has “peculiar powers” in the area of foreign affairs despite the importance of national security concerns, the decision of whether a search is

~~SECRET~~

~~SECRET~~

justified must be "made by a neutral and disinterested magistrate or judge rather than by an executive official," *id.* at 614-16.

Both *Keith* and *Zweibon* recognized that even weighty national security threats cannot justify entrusting the fundamental rights of American citizens to the discretion of one branch of government. The *Keith* court found that the involvement of the judiciary not only ensures the protection of those subject to executive exercises of power, but it serves a more general societal purpose, namely, to reassure the public generally that "indiscriminate wiretapping and bugging of law abiding citizens cannot occur." *Keith*, 407 U.S. at 321. The PAA does precisely the opposite – it creates a widespread perception that "indiscriminate wiretapping and bugging" can and will occur. By vesting too much discretion in the executive branch and eliminating the fundamental role of the judiciary in approving surveillance directed against U.S. citizens, the PAA brings about the very harm the *Keith* court sought to forestall when it refused to create a warrant exception for national security interests.

The justification for a foreign intelligence exception is even less compelling now than it was at the time of *Keith*. After *Keith*, Congress addressed the practical concerns raised by the government in *Keith* by passing FISA. Now, the FISA process provides a speedy, secret mechanism for the government to obtain prior judicial authorization for surveillance and searches from a specially-created court with expertise in addressing national security concerns. In light of this available substitute for Title III Orders, a categorical warrant exception is unnecessary.

b) The PAA is Inconsistent with Any Decision Recognizing a Foreign Intelligence Exception

Even if this court were to follow pre-FISA case law recognizing the possibility of a constitutionally-valid foreign intelligence exception to the warrant requirement, the PAA does not

~~SECRET~~

~~SECRET~~

satisfy the standard for the applicability of such an exception because the surveillance permitted under the PAA is not carefully limited in scope to the acquisition of foreign intelligence.

The courts outside the FISC that have recognized a foreign intelligence exception to the warrant requirement have done so only under circumstances not present here. In *United States v. Truong Dinh Hung*, the Fourth Circuit recognized that "because individual privacy interests are severely compromised any time the government conducts surveillance without prior judicial approval, this foreign intelligence exception to the Fourth Amendment warrant requirement must be carefully limited to those situations in which the interests of the executive are paramount." *United States v. Truong Dinh Hung*, 629 F.2d 908, 915 (4th Cir. 1980). Specifically, the court held that the warrant requirement should only be excused if "the object of the search or the surveillance is a foreign power, its agent or collaborators," and if "the surveillance is conducted 'primarily' for foreign intelligence reasons." *Id.* In *United States v. Butenko*, the Third Circuit adopted a slightly different standard, allowing an exception to the warrant requirement for surveillance that was "conducted and maintained *solely* for the purpose of gathering foreign intelligence." *United States v. Butenko*, 494 F.2d 593, 605 (3rd Cir. 1974) (emphasis supplied).

Under either test, the Directives would fail to qualify for a foreign intelligence exception to the warrant requirement. First, the surveillance authorized is not limited to "a foreign power, its agent or collaborators" but rather can target U.S. citizens if they are "reasonably believed to be located outside of the United States," regardless of their affiliation with an foreign power (or lack thereof). 50 U.S.C. § 1805b(a). Second, the surveillance need not be "solely" or even "primarily" for foreign intelligence purposes, so long as "a significant purpose of the acquisition is to obtain foreign intelligence information." 50 U.S.C. § 1805b(a)(4). In short, the PAA authorizes surveillance of any person reasonably believed to be located outside the U.S., whether or not connected to a foreign power, for any reason, including the needs of ordinary law enforcement, provided the surveillance also has a "significant" foreign intelligence purpose. Although the FISC

- 16 -

~~SECRET~~

~~SECRET~~

in *In re Sealed Case* determined that the “significant” foreign intelligence purpose was sufficient to pass constitutional muster, it did so only in the context of a target who had been identified as a foreign power or an agent of a foreign power. *See* 310 F.3d at 720. It is unclear that the FISCR would have reached the same conclusion where the “significant” purpose test is applied to a U.S. citizen who is not an agent of a foreign power.<sup>12</sup>

The grounds for finding a foreign intelligence exception are weaker now than in *Truong* and *Butenko* because those decisions involved pre-FISA surveillance, when the only alternative to a warrant exception was the Title III process for obtaining a wiretap order. Specifically, in *Truong*, one ground for allowing an exception was that requiring a warrant would (a) frustrate the executive’s need for speed and secrecy; and (b) would require the judiciary to act in an area in which it does not have expertise. *Truong*, 629 F.2d at 913-14.<sup>13</sup> Similarly, in *Butenko*, the court found that an exception to the warrant requirement was appropriate, in part, because of the need for the executive to act “secretly and quickly.” *Butenko*, 494 F.2d at 605. These concerns are no longer persuasive given the availability of the FISA process.

c) No Other Exceptions to the Warrant Requirement Apply

Of the other “specifically established and well-delineated exceptions” to the warrant requirement, *Katz*, 389 U.S. at 357, the only one that arguably could apply here is the “special needs” doctrine, which authorizes warrantless searches that are undertaken for purposes beyond the normal need for law enforcement. Nevertheless, the PAA does not qualify for any of those narrowly drawn exceptions to the warrant requirement.

<sup>12</sup> A district court recently reached a different conclusion as to the constitutionality of the “significant” purpose test, even with regard to an agent of a foreign power, contending that the FISCR’s constitutional analysis was erroneous. *See Mayfield v. United States*, 504 F. Supp. 2d 1023, 1041-42 (D. Or. 2007) (holding FISA unconstitutional to the extent it authorizes searches with only a “significant” foreign intelligence gathering purpose).

<sup>13</sup> *Id.* at 913 n. 2 (recognizing that the practical difficulties of obtaining a warrant for foreign intelligence surveillance were particularly acute because prior judicial authorization surveillance could only have occurred under Title III as FISA was not yet in effect).

~~SECRET~~



~~SECRET~~

First, the “special needs” cases typically involve situations where there is a limited search or a reduced expectation of privacy, not cases—like this one—that involve the surveillance of private communications.<sup>14</sup> Here there is neither a lower expectation of privacy, nor a limited search. The search commanded by the Directives involves [REDACTED]

[REDACTED] (Mot. to Compel, Ex. 1 at 2). Second, “special needs” cases typically involve situations where the execution of the search involves little discretion, as opposed to the surveillance here which is trusted to the sole discretion of the executive branch, especially with regard to its ability to target unlimited numbers of individuals for up to one year. See *United States v. Brignoni-Ponce*, 422 U.S. 873, 882 (1975) (refusing to apply special needs to search that was “solely at the discretion of Border Patrol officers”). Third, because the Directives potentially authorize ordinary law enforcement surveillance that also has a foreign intelligence purpose, it is not narrowly directed at a “special need.” See *Mayfield*, 504 F. Supp. 2d at 1042 (finding “special needs” exception inapplicable to FISA because FISA surveillance “may have as its ‘programmatic purpose’ the generation of evidence for law enforcement purposes”); *City of Indianapolis v. Edmond*, 531 U.S. 32, 48 (2000) (holding that where government’s *primary* purpose is to uncover evidence of criminal wrongdoing, a highway checkpoint did not fit within special needs exception).

Finally, if the government argues that the President has inherent authority under Article II of the U.S. Constitution to conduct surveillance of U.S. citizens for foreign intelligence purposes, that authority does not obviate the need for this Court to consider the Fourth Amendment rights of United States citizens.<sup>15</sup> In enlisting this Court to compel Yahoo! to comply with the Directives, the government is relying on the procedures of the PAA, which—like all legislative enactments—must

<sup>14</sup> See, e.g., *Terry v. Ohio*, 392 U.S. 1 (1968) (stop-and-frisk); *United States v. Martinez-Fuerte*, 428 U.S. 543 (1976) (border searches); *Bell v. Wolfish*, 441 U.S. 520 (1979) (prisons); *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646 (1995) (student drug tests).

<sup>15</sup> Even if the President has such authority, it still must be exercised consistent with the “reasonableness” requirements of the Fourth Amendment. See *Truong*, 629 F.2d at 916 (applying Fourth Amendment analysis to surveillance authorized by the President); *Butenko*, 494 F.2d at 603 (“the Fourth Amendment is also applicable where, as here, the President is acting pursuant to his foreign affairs duties”).

~~SECRET~~



~~SECRET~~

meet Fourth Amendment requirements. See *In re Sealed Case*, 310 F.3d at 736 ("we are obliged to consider whether the [FISA] statute as amended is consistent with the Fourth Amendment").

#### 4. *The Directives Require Unreasonable Searches*

Even if the searches required by the Directives do not require an actual warrant, they must meet the reasonableness requirements of the Fourth Amendment. The existence of an exception to the warrant requirement—even on the grounds of national security—does not allow the Fourth Amendment to be ignored. "[A]ssuming *arguendo* that FISA orders are not Fourth Amendment warrants, the question becomes, are the searches constitutionally reasonable." *In re Sealed Case*, 310 F.3d at 744; see also *Truong*, 629 F.2d at 916 ("Even if a warrant is not required, the Fourth Amendment requires that the surveillance be 'reasonable'").

In the only opinion ever issued by the FISC, the court addressed whether a FISC order authorizing surveillance pursuant to pre-PAA sections of FISA satisfied the Fourth Amendment. 310 F.3d at 717. The FISC did not decide whether such an order constituted a "warrant," but concluded that, even if it did not, the procedures for obtaining such an order satisfied the "reasonableness" requirement of the Fourth Amendment. *Id.* at 746. The FISC believed that a useful way of approaching the question of reasonableness was to determine how closely the relevant procedures approximate the requirements for a warrant under Title III.<sup>16</sup> *Id.* at 737 ("obviously, the closer those FISA procedures are to Title III procedures, the lesser are [the] constitutional concerns").<sup>17</sup> In making the comparison to the Title III procedures, the Court observed that

<sup>16</sup> Several courts have recognized that the core elements of Title III, namely, (a) probable cause, (b) particularity of description, (c) necessity of means employed, (d) limited duration, and (e) minimization, embody the requirements of the Fourth Amendment. See, e.g., *United States v. Falls*, 34 F.3d 674, 680 (8th Cir. 1994) (looking to Title III for "guidance in implementing the Fourth Amendment with regard to video surveillance"); *United States v. Mesa-Rincon*, 911 F.2d 1433, 1438 (10th Cir. 1990) (looking to Title III "for guidance in implementing the fourth amendment in an area that Title III does not specifically cover"); *United States v. Biasucci*, 786 F.2d 504, 510 (2d Cir. 1986) ("we borrow the statutory standards quoted above [from Title III] as a measure of the government's constitutional obligation").

<sup>17</sup> The FISC's reasoning follows the Court's observation that Fourth Amendment "'reasonableness' derives content and meaning through reference to the warrant clause." *Keith*, 407 U.S. at 309-10.

~~SECRET~~

~~SECRET~~

“beyond requiring searches and seizures to be reasonable, the Supreme Court has interpreted the warrant clause to require three elements,” namely, (a) issuance by a neutral magistrate, (b) a showing of probable cause, and (c) particularity. *Id.* at 737-38. In concluding that the procedures and government showings required under FISA came close to meeting the Fourth Amendment standards the Court found the following factors important:

- prior judicial scrutiny, *id.* at 738;
- court reviewable certification that the information sought is “foreign intelligence information,” *id.*;
- showing of probable cause that the target is a “foreign power or agent of a “foreign power,” *id.*;
- showing of probable cause that the facilities or places at which the surveillance is directed are being used, or are about to be used, by a foreign power or agent, *id.* at 739-40;
- necessary that the information is not available through normal investigative procedures, *id.*;
- orders are limited to 90 days, *id.*; and
- minimization, *id.*

Only one of these factors—minimization—is present in the PAA. More specifically:

- The PAA mandates no prior review of any part of the directive—the limited review of the procedures mandated by Section 105C need not be completed until February 2008, but the Directives are effective immediately, 50 U.S.C. § 1805c(b);
- the limited review provided by the PAA is only a review of the procedures set forth for determining the likely location of the target, and is not a review of the type of information sought, 50 U.S.C. § 1805c;
- no showing of probable cause is ever required by the PAA;
- no showing regarding necessity of using the PAA’s procedures is ever required by the PAA;
- once a Section 105B certification is made, it is valid for an entire year, 50 U.S.C. § 1805b(a).

Here, the procedures of the PAA do not approximate the three elements mandated by the warrant clause, and are not “close” to meeting the reasonableness requirements of the Fourth

~~SECRET~~

~~SECRET~~

Amendment. *See also Mincey v. Arizona*, 437 U.S. 385, 393 (1978) (“warrantless search must be ‘strictly circumscribed by the exigencies which justify its initiation’”). Instead the PAA imposes few limitations on the executive branch, and fails to achieve “the essential purpose of the proscriptions in the Fourth Amendment [which] is to impose a standard of ‘reasonableness’ upon the exercise of discretion by government officials, including law enforcement agents, in order to safeguard the privacy and security of individuals against arbitrary invasions.” *Delaware v. Prouse*, 440 U.S. 648, 653-54 (1979) (internal quotations omitted).

The “reasonableness” analysis of *In re Sealed Case*, dictates the conclusion that to the extent that surveillance required by the Directives and authorized by the PAA captures the communications of United States citizens who are not agents of foreign powers, the surveillance is not reasonable under the Fourth Amendment.

C. The PAA Violates the Separation of Powers and is Otherwise Flawed

The Directives are the product of the PAA’s certification process, which, as explained above, falls well short of the requirements of the Fourth Amendment, in part because of the lack of sufficient judicial review. In fact, the PAA’s limitations on judicial review imposes constitutionally impermissible restrictions on the judicial branch. Congress cannot legislate a constitutional standard of review that contradicts or supercedes what the courts have determined to be the appropriate level of judicial scrutiny. *See Doe v. Gonzales*, 500 F. Supp. 2d 379, 411 (S.D.N.Y. 2007) (concluding statute regarding disclosure of NSLs violated separation of powers because it imposed standard of review different than the standard applicable under the First Amendment). Accordingly, it is a separation of powers violation if a statute attempts to force courts to deviate from judicially determined “constitutional rules.” *Id.* at 413. That, however, is exactly what the PAA appears to do, violating the constitutional requirement of separation of powers.

First, the PAA provides only for judicial review of the government’s procedures for ensuring that acquisitions conducted pursuant to section 105B do not constitute electronic

~~SECRET~~

~~SECRET~~

surveillance and that review is "limited to whether the Government's determination is clearly erroneous." 50 U.S.C. § 1805c(b). By contrast, the Fourth Amendment requires courts to consider whether a particular search is "reasonable," and "there can be no ready test for determining reasonableness other than by balancing the need to search against the invasion which the search entails." *Camara v. Mun. Court*, 387 U.S. 523, 536-37 (1967). That balancing cannot be accomplished by a court that is only permitted to review for "clear error."<sup>18</sup>

Second, the court's ability to conduct the balancing needed to make a reasonableness determination is seriously constrained by the fact that it cannot evaluate the actual Section 105B(a) certification. In particular, it cannot review the government's determination that the information sought to be acquired is in fact "not electronic surveillance" or that a "significant purpose of the acquisition is to obtain foreign intelligence information." 50 U.S.C. § 1805b(a). Without such authority, the court is not in a position to balance the "need to search," against the "invasion which the search entails" as required by the Fourth Amendment. *Camara*, 387 U.S. at 536-37; *see also Berger*, 388 U.S. at 56 ("need for particularity and evidence of reliability . . . is especially great in the case of eavesdropping")

In *Doe*, the court warned of the danger of legislative incursions into the province of the judiciary when addressing a statute that similarly constrained judicial review of NSLs issued under 18 U.S.C. § 2709:

Of greatest concern, the law encroaches onto what is perhaps the most consequential authority the courts possess: the sole power to judge how to take the proper measure of the validity of a statute as aligned against the precepts of the Constitution itself, and to that end decide what constitutional rule of law must apply to guide that crucial test. Thus, this aspect of the Reauthorization Act, however legitimate and compelling the national interests it otherwise embodies, fails a test of recognition, insofar as it breaches the proper constitutional limits drawn for our government by the concepts of separation and balance of power. . . . All could be lost of the judiciary's most vital function, and hence of the individual freedoms of Americans, if the courts

<sup>18</sup> In considering the instant motion, however, this Court is not so limited. Section 105B(g) permits this Court to review the Directive to determine if it is "otherwise lawful." 50 U.S.C. § 1805b(g).

~~SECRET~~

~~SECRET~~

were to cede fundamental decisional power to Congress, and were Congress in turn empowered to override the courts in laying down the law that governs constitutional review of legislation or of an action of the executive.

500 F.Supp.2d at 411. Here, as in *Doe*, the dictated standard of review interferes with the vital role of the judiciary to ensure that the Constitution, as interpreted by the courts, remains the supreme law of the land. See *Marbury v. Madison*, 5 U.S. 137, 177 (1803) ("it is emphatically the province and the duty of the judicial department to say what the law is.").

Furthermore, the PAA is defective insofar as the provisions in section 105C of FISA requiring judicial review of the government's determination that its procedures are "reasonably designed to ensure that the acquisitions conducted pursuant to [section 105B] do not constitute electronic surveillance" do not match the language of section 105B(a)(1) which requires the government to certify "that are reasonable procedures in place for determining that the acquisition . . . concerns persons reasonably believed to be located outside the United States" Compare 50 U.S.C. § 1805b(a)(1) with 50 U.S.C. § 1805c(b).<sup>19</sup> There is no mention in section 105B of the creation or submission to the FISC of the procedures that the Court is intended to review under section 105C. In light of this ambiguity, it is unclear what should be submitted to, and reviewed by, this Court.

The statute is problematic for two additional reasons. It is Yahoo!'s understanding that the Court has not approved the procedures required to be submitted to it under §1805c(a), and is not required to do so before February 2008. Yet the Directives are effective immediately. Yahoo! should not be required to comply with the Directives until this Court has approved the government's procedures, because the judiciary's "independent check upon executive discretion is not satisfied . . . by 'extremely limited' post-surveillance judicial review." *Keith*, 407 U.S. 297, at 317-18.

<sup>19</sup> The two things are not identical. Surveillance that "concerns persons reasonably believed to be located outside the United States" is not the same as surveillance that "does not constitute electronic surveillance" because the latter definition only covers communications "directed at persons reasonably believed to be located outside the United States." Thus, surveillance that concerns persons outside the U.S. may nevertheless qualify as electronic surveillance if it is not also directed at persons outside the U.S., e.g., a phone call between U.S. persons about a person outside the U.S.

~~SECRET~~

~~SECRET~~

In addition, the Directives require compliance for up to one year. Although the PAA purports to provide Yahoo! with immunity for complying with a directive, *see* U.S.C. § 1805b(1), the PAA -- including the immunity provision -- sunsets in February 2008, *see* PAA §6(c). Thus, there is a possibility that the immunity provisions of the PAA designed to protect providers like Yahoo! may not apply beyond the sunset of the statute.<sup>20</sup>

D. The Directives Improperly Implement the PAA

Even if the PAA is constitutional, the Directives are inconsistent with the PAA to the extent that they require Yahoo! to intercept the communications of any persons the government might identify over the next year. Compelling Yahoo! to capture communications of persons not known at the time of the certification filed with the FISC bypasses the few provisions of the PAA that limit the AG and DNI's ability to conduct surveillance activities.

The Directives do not identify any specific persons targeted by the intended acquisition. Rather, the Directives specifically require Yahoo! to implement surveillance against whatever users the government may identify in the future, even if such persons were unknown to the government at the time of certification to the FISC. This leaves the identification of targeted persons to the government's discretion and is inconsistent with the certification requirements of the PAA.

As a statutory matter, the PAA requires the government, through the DNI and the AG, to certify to the FISA court that the planned interception "does not constitute electronic surveillance." 50 U.S.C. § 1805b(a)(2). If the key part of the certification is that the targeted persons are reasonably believed to be outside the U.S., this requirement cannot be met for individuals that were not yet identified by the government at the time the certifications were filed. Logically, the certifications require the government to know the individuals and their location. Without such knowledge, all the government can certify in advance is that there are reasonable procedures in

---

<sup>20</sup> A FISC Order would carry with it immunity from liability pursuant to 50 U.S.C. §1805(i) as well as 18 U.S.C. § 2511(2)(a)(ii).

~~SECRET~~

~~SECRET~~

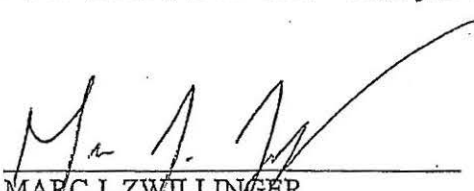
place for determining that the individual users *will be* located outside the U.S. at the time they are specified to the provider.<sup>21</sup> But the certification that the specific acquisition "does not constitute electronic surveillance" must have an additional meaning beyond describing the procedures required by (a)(1) or it would be entirely superfluous.

In other words, the PAA appears to contemplate that the government's certification address both procedures and outcome. The government must certify that it has sound procedures in place, *and*, as the result of applying those procedures, the acquisition it intends to conduct "does not constitute electronic surveillance," such that it does not require a FISA order. 50 U.S.C. § 1805b(a)(2). Although a certification under the PAA "is not required to identify the specific facilities, places, premises or property at which the acquisition of the foreign intelligence information will be directed," the statute does not suggest that the universe of targeted persons can be expanded after the certifications are filed. That is what the Directives served upon Yahoo! allow. As such, they are inconsistent with the PAA.

### CONCLUSION

For the foregoing reasons, Yahoo! respectfully requests that this Court deny the government's Motion to Compel and order such other relief as the Court deems just and proper.

DATED: November 30, 2007

  
MARC J. ZWILLINGER  
Sonnenschein Nath & Rosenthal LLP  
1301 K Street, N.W.  
Suite 600; East Tower  
Washington, DC 20005  
Tel: (202) 408-6400  
Fax: (202) 408-6399  
mzwillinger@sonnenschein.com  
*Attorneys for Yahoo! Inc.*

<sup>21</sup> This certification requirement is required by 50 U.S.C. § 1805b(a)(1).

~~SECRET~~




~~SECRET~~

## CERTIFICATE OF SERVICE

I hereby certify that on this 30<sup>th</sup> day of November, 2007, I provided a true and correct copy of Yahoo! Inc.'s Memorandum in Opposition to Motion to Compel (the "Opposition") to an agent designated by the Court Security Officer, who has informed me that he will deliver one copy of the Opposition to the Court for filing, and a second copy to the:

United States Department of Justice  
National Security Division  
950 Pennsylvania Ave., NW  
Room 6150  
Washington, D.C. 20530



MARC J. ZWILLINGER  
Sonnenschein Nath & Rosenthal LLP  
1301 K Street, N.W.  
Suite 600; East Tower  
Washington, DC 20005  
Tel: (202) 408-6400  
Fax: (202) 408-6399  
mzwillinger@sonnenschein.com  
*Attorneys for Yahoo!, Inc.*

~~SECRET~~