UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE DIRECTIVES TO YAHOO!, INC. PURSUANT TO SECTION 105B OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT ~~(S)~~

Docket Number 105B(g): 07-01 ~~(S)~~

MEMORANDUM OPINION (U)

Background (U)

This case comes before the Court on the government's motion to compel compliance with directives it issued to Yahoo!, Inc. (Yahoo) pursuant to the Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (PAA), which was enacted on August 5, 2007. The PAA amended the Foreign Intelligence Surveillance Act (FISA) (which, in its present form, can be found at 50 U.S.C.A. §§ 1801-1871 (West 2003, Supp. 2007 & Oct. 2007)), by creating a new framework for the collection of foreign intelligence information concerning persons reasonably believed to be outside of the United States. Under the PAA, the Attorney General and the Director of National Intelligence may authorize the acquisition of such information for periods of up to one year pursuant to a "certification" that satisfies specific statutory criteria, and may direct third parties to assist in such acquisition. 50 U.S.C.A. §§ 1805a - 1805c. ~~(S)~~

Subsequent to the passage of the PAA, the Attorney General and the Director of National Intelligence, pursuant to 50 U.S.C.A. § 1805b(a), executed [redacted] certifications that authorized the acquisition of certain types of foreign intelligence information concerning persons reasonably believed to be outside the United States.[1] In furtherance of these acquisitions, in [redacted] 2007, the Attorney General and the Director of National Intelligence issued [redacted] directives to Yahoo. Feb. 2008 Classified Appendix at [redacted] Yahoo refused to comply

---

[redacted]

[2] Each directive states that

> [t]he Government will [redacted] pursuant to the above-referenced Certification in a mutually agreed upon format. [redacted]

(continued...)

with the directives, and on November 21, 2007, the government filed a motion asking this Court to compel Yahoo's compliance. Motion to Compel Compliance with Directives of the Director of National Intelligence and Attorney General (Motion to Compel). Yahoo responded by contending that the directives should not be enforced because they violate both the PAA and the Fourth Amendment. Yahoo also contends that the PAA violates separation of powers principles and is otherwise flawed. ~~(S)~~

Extensive briefing followed on this complicated matter of first impression. Yahoo has raised numerous statutory claims relating to the PAA, which is hardly a model of legislative clarity or precision. Yahoo's principal constitutional claim relates to the Fourth Amendment rights of its customers and other third parties, and raises complex issues relating to both standing and substantive matters. Furthermore, additional issues have arisen during the pendency of the litigation. For one thing, most of the PAA has sunset, raising the issue of whether this Court retains jurisdiction over the government's motion to compel. For another, the government filed a classified appendix with the Court in December 2007,[3] which contained the certifications and

---

[2](...continued)

> [redacted] . . . is hereby directed . . . to immediately provide the Government with all information, facilities, and assistance necessary to accomplish this acquisition in such a manner as will protect the secrecy of the acquisition and produce a minimum of interference with the services that Yahoo provides.

Feb. 2008 Classified Appendix at [redacted] ~~(S)~~

[3] This classified appendix was filed ex parte, pursuant to 50 U.S.C.A. § 1805b(k). Yahoo did not object to the ex parte filing of this initial classified appendix. Pursuant to section (continued...)

procedures underlying the directives, but the government then inexplicably modified and added to those certifications and procedures [redacted] required this Court to order additional briefing and consider additional statutory issues, such as whether the PAA authorizes the government to amend certifications after they are issued, and whether the government can rely on directives to Yahoo that were issued prior to the amendments.[4] (S)

For the reasons set forth below, the Court holds that it retains jurisdiction over the government's motion to compel, and that the motion is in fact meritorious. The Court also finds that the directives issued to Yahoo comply with the PAA and with the Constitution. A separate Order granting the government's motion is therefore being issued together with this Opinion. (S)

Part I of this Opinion explains why the expiration of much of the PAA does not deprive the Court of jurisdiction over the government's motion. Part II of this Opinion rejects the statutory challenges advanced by Yahoo, and concludes that the directives in this case comply with the PAA and are still in effect pursuant to the amended certifications. Part II also rejects Yahoo's separation of powers challenge to the PAA. Part III of the Opinion holds that Yahoo

---

[3](...continued)
1805b(k), the Court subsequently allowed the government to file, ex parte, the updated, February 2008 classified appendix. Although Yahoo requested a copy of that appendix redacted to the level of the security clearance held by Yahoo's counsel, section 1805b(k) does not require, and the Court did not order, the government to provide such a document to Yahoo. (S)

[4] The Court's February 29, 2008 Order Directing Further Briefing on the Protect America Act lays out in greater detail the circumstances that required the additional briefing. (S)

may in fact raise the Fourth Amendment rights of its customers and other third parties, but further holds that the directives to Yahoo comply with the Fourth Amendment because they fall within the foreign intelligence exception to the warrant requirement and are reasonable. (S)

Analysis (U)

I. The Court Retains Jurisdiction Over the Motion to Compel Notwithstanding the Lapse of the PAA. (S)

As originally enacted, the PAA had a "sunset" provision, under which its substantive terms would "cease to have effect 180 days after the date of the enactment" of the PAA, subject to exceptions discussed below. PAA § 6(c). On January 31, 2008, Congress extended this period to "195 days after the date of the enactment of [the original PAA]." See Pub. L. 110-182, § 1, 122 Stat. 605. Congress took no further action, and this 195-day period expired on February 16, 2008. Yahoo argues that this statutory lapse deprives this Court of jurisdiction to entertain the government's motion to compel. Yahoo's Supplemental Briefing on PAA Statutory Issues (Yahoo's Supp. Brief. on Stat. Issues) at 13-16. For the following reasons, the Court finds that it retains jurisdiction by virtue of section 6(c) of the PAA. (S)

Section 2 of the PAA amended FISA by adopting additional provisions, codified at 50 U.S.C.A. §§ 1805a and 1805b. One of the provisions added to FISA by section 2 of the PAA states as follows:

> In the case of a failure to comply with a directive issued pursuant to subsection (e), the Attorney General may invoke the aid of the [Foreign Intelligence Surveillance Court (FISC)] to compel compliance with the directive. The court shall issue an order requiring the person to comply with the directive if it finds that the directive was issued in accordance with subsection (e) and is otherwise lawful.

PAA § 2 (codified at 50 U.S.C.A. § 1805b(g)). Unquestionably, this provision gave the Court jurisdiction over the government's motion prior to February 16, 2008. (U)

Section 6 of the PAA, as amended, states in relevant part:

> (c) SUNSET.–Except as provided in subsection (d), sections 2, 3, 4, and 5 of this Act, and the amendments made by this Act, shall cease to have effect 195 days after the date of the enactment of this Act.
>
> (d) AUTHORIZATIONS IN EFFECT.–Authorizations for the acquisition of foreign intelligence information pursuant to the amendments made by this Act, and directives issued pursuant to such authorizations, <u>shall remain in effect until their expiration</u>. Such acquisitions shall be governed by the applicable provisions of such amendments and shall not be deemed to constitute electronic surveillance as that term is defined in [50 U.S.C.A. § 1801(f)].

PAA § 6, as amended by Pub. L. 110-182, § 1, 122 Stat. 605 (emphasis added). Yahoo concedes that under the first sentence of § 6(d), the directives remain in effect. Yahoo's Supp. Brief. on Stat. Issues at 14. However, Yahoo contends that § 6(d) does not preserve this Court's jurisdiction over the government's motion to compel compliance with the directives it received. On the other hand, the government posits that the second sentence of § 6(d) – providing that "[s]uch acquisitions shall be governed by the applicable provisions of such amendments" – preserves the Court's jurisdiction. United States of America's Supplemental Brief on the Fourth Amendment (Govt.'s Supp. Brief on the Fourth Amend.) at 10 n.8. (S)

The Court begins its analysis of the parties' conflicting views by examining the controlling statutory text. In the second sentence of § 6(d), the phrase "[s]uch acquisitions" plainly refers to acquisitions conducted pursuant to the "[a]uthorizations for the acquisition of foreign intelligence information pursuant to the amendments made" by the PAA, "and directives issued pursuant to such authorizations," both which "remain in effect" under the immediately preceding sentence. The second sentence of § 6(d) provides that those acquisitions "shall be governed by the applicable provisions of such amendments." Here too, the phrase "such amendments" refers to the "amendments" in the immediately preceding sentence – i.e., the amendments made by the PAA, pursuant to which the acquisition of foreign intelligence information has been authorized. Thus, acquisitions that remain authorized under the first sentence of § 6(d) shall, by virtue of the second sentence, be governed by the "applicable" provisions of those amendments. (U)

The relevant question under § 6(d) therefore becomes whether the provision of the PAA codified at § 1805b(g) is fairly understood to be part of those PAA amendments pursuant to which the relevant acquisitions were authorized, and which are "applicable" to those acquisitions. If so, then section 6(d) operates to maintain the applicability of § 1805b(g) with regard to the directives issued to Yahoo, thereby preserving the Court's jurisdiction to enforce those directives. The structure and logic of the amendments enacted by the PAA strongly support the conclusion that section 6(d) has this effect. (S)

Section 2 of the PAA added to FISA all of the provisions codified at 50 U.S.C.A. §§ 1805a and 1805b in the form of a single, comprehensive amendment.[5] Section 1805b (which is titled "Additional Procedure for Authorizing Certain Acquisitions Concerning Persons Located Outside of the United States") provides a comprehensive framework for the authorization and conduct of certain acquisitions of foreign intelligence information. In addition to § 1805b(g),

[5] "The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by inserting after [50 U.S.C.A. § 1805] the following: [the full text of §§ 1805a and 1805b follows]." PAA § 2. (U)

this framework includes a grant of authority to the Attorney General and the Director of National Intelligence, "[n]othwithstanding any other law," to authorize such acquisitions, subject to specified procedural and substantive requirements (i.e., § 1805b(a), (c), (d)); authority to "direct" a person, such as Yahoo, to assist in such acquisition (i.e., § 1805b(e)); immunity from civil liability for providing assistance in accordance with such a directive (i.e., § 1805b(l)); a mechanism by which a person who has received such a directive may challenge its legality before the FISC (i.e., § 1805b(h)), with an ability to appeal to the Foreign Intelligence Surveillance Court of Review (i.e., § 1805b(i)); and procedural and security requirements for judicial proceedings under § 1805b (i.e., § 1805b(j), (k)). Thus, § 1805b(g) constitutes one part of the integrated statutory framework codified by § 1805b for authorizing the acquisition of foreign intelligence information. It is therefore no stretch to regard § 1805b(g) as included within "the amendments" pursuant to which the relevant acquisitions were authorized, and as "applicable" to those acquisitions. Indeed, that is the natural construction of the terms of § 6(d) as applied to § 1805b(g). (S)

Yahoo takes the view that § 6(d) does not preserve the efficacy of § 1805b(g) with regard to directives that had not been complied with at the time that the PAA expired. Yahoo's Supp. Brief. on Stat. Issues at 14. But as explained above, nothing in the language of § 6(d) supports this result. The phrase "[s]uch acquisitions" in the second sentence of § 6(d) plainly refers to the description, in the immediately preceding sentence, of acquisitions authorized pursuant to amendments made by the PAA. And, the preserving language in the second sentence is not limited to acquisitions both authorized pursuant to amendments made by the PAA and actually occurring before the PAA's expiration date. (S)

However, assuming arguendo that this statutory language might also reasonably bear the interpretation that § 1805b(g) is not preserved by § 6(d) for purposes of the directives issued to Yahoo, the Court would then have to assess which interpretation would serve the purposes envisioned by Congress.[6] Without doubt, Congress intended for the FISC to have jurisdiction over § 1805b(g) actions to compel compliance with directives prior to the expiration date for the PAA specified in § 6(c). It is equally clear that, even after that expiration date, the challenged directives "remain in effect until their expiration." § 6(d). There is no discernible reason why Congress would have chosen to dispense with the forum and process that it specifically established to compel compliance with lawfully issued directives, while providing that the directives themselves remain in effect. And the particular interpretation advanced by Yahoo yields the inexplicable outcome that recipients who have never complied with directives are now beyond the reach of § 1805b(g)'s enforcement mechanism, but recipients who were compliant as of February 16, 2008, would still be subject to it. The "illogical results of applying such an interpretation . . . argue strongly against the conclusion that Congress intended" such divergent

[6] See, e.g., Jones v. R.R. Donnelley & Sons Co., 541 U.S. 369, 377 (2004) (ambiguous statute interpreted in view of "the context in which it was enacted and the purposes it was designed to accomplish"). (U)

results when it enacted § 6(d). Western Air Lines, Inc. v. Board of Equalization of the State of South Dakota, 480 U.S. 123, 133 (1987).[7] (S)

In support of its interpretation, Yahoo cites authority which concludes that the repeal of a jurisdiction-conferring statute deprives a court of jurisdiction over pending cases, in the absence of a clause in the repealing statute that preserves jurisdiction.[8] But the PAA includes a preservation clause, see § 6(d), and the issue in this case is how broadly or narrowly that clause should be construed. The authority cited by Yahoo does not shed light on that issue. (S)

Yahoo also suggests that De La Rama S.S. Co. v. United States, 344 U.S. 386 (1953), requires that Congress employ "plain terms" to preserve jurisdiction over pending cases when the statute previously conferring jurisdiction is repealed. Yahoo's Supp. Brief. on Stat. Issues at 15. But De La Rama does not enunciate an unqualified "plain statement" requirement. Instead, in

---

[7] Yahoo cites several statements from congressional debate on the PAA that emphasize that the PAA was a temporary statute, set to expire in six months (subsequently extended by 15 days, as noted above). Yahoo's Supp. Brief. on Stat. Issues at 16 (quoting, e.g., 153 Cong. Rec. H9958-59 (daily ed. Aug. 4, 2007) (statement of Rep. Issa) ("[W]hat we're doing is passing a stopgap 6-month, I repeat, 6-month bill. This thing sunsets in 6 months.")). But the statements cited by Yahoo, of which Rep. Issa's statement is illustrative, shed no light on the interpretative issue presented, which is the intended scope of §6(d)'s exception from the general sunset provision. Indeed, the statements quoted by Yahoo do not even acknowledge the existence of any exceptions to the PAA's sunset provision. (S)

[8] Yahoo's Supp. Brief. on Stat. Issues at 15 (citing Bruner v. United States, 343 U.S. 112, 116-17 (1952); Santos v. Guam, 436 F.3d 1051, 1052 (9th Cir. 2006); United States v. Stromberg, 227 F.3d 903, 907 (5th Cir. 1955)). (S)

the context of interpreting the general savings statute in 1 U.S.C. § 109 (2000),[9] the De La Rama Court observed:

> The Government rightly points to the difference between the repeal of statutes solely jurisdictional in their scope and the repeal of statutes which create rights and also prescribe how the rights are to be vindicated. In the latter statutes, "substantive" and "procedural" are not disparate categories; they are fused components of the expression of a policy. When the very purpose of Congress is to take away jurisdiction, of course it does not survive, even as to pending suits, unless expressly reserved . . . But where the object of Congress was to destroy rights in the future while saving those which have accrued, to strike down enforcing provisions that have special relation to the accrued right and as such are part and parcel of it, is to mutilate that right and hence to defeat rather than further the legislative purpose.

344 U.S. at 390 (emphasis added). Applying this principle, the De La Rama Court found that jurisdiction over pending cases was preserved, despite the repeal of the statute originally conferring jurisdiction. Id. at 390-91. (S)

---

[9] This provision, which has not been amended since 1947, states:

> The repeal of any statute shall not have the effect to release or extinguish any penalty, forfeiture, or liability incurred under such statute, unless the repealing Act shall so expressly provide, and such statute shall be treated as still remaining in force for the purpose of sustaining any proper action or prosecution for the enforcement of such penalty, forfeiture, or liability. The expiration of a temporary statute shall not have the effect to release or extinguish any penalty, forfeiture, or liability incurred under such statute, unless the temporary statute shall so expressly provide, and such statute shall be treated as still remaining in force for the purpose of sustaining any proper action or prosecution for the enforcement of such penalty, forfeiture, or liability. (U)

1 U.S.C. § 109. Because the Court finds that § 6(d), the PAA's specific savings clause, serves to preserve jurisdiction over the government's action to enforce the directives issued to Yahoo, it is not necessary to consider whether this general savings clause would support the same conclusion. (S)

In this case, the jurisdictional, procedural, and substantive provisions of § 1805b are fairly regarded as "fused components of the expression of a policy" that Congress adopted when it enacted the PAA. To the extent De La Rama bears on this case, it counsels against the interpretation advanced by Yahoo. (S)

For the above-described reasons, the Court finds that it retains jurisdiction over the government's motion to compel compliance with the directives issued to Yahoo, by virtue of § 6(d)'s preservation of § 1805b(g) with regard to the directives that the government seeks to enforce against Yahoo. (S)

II. The Yahoo Directives Comply With the PAA and Can Be Enforced Without Violating the Constitutional Separation of Powers Doctrine. (S)

A. Compelling Compliance With the Directives Under the PAA Does Not Violate Separation of Powers Principles. (S)

Yahoo argues that the PAA is unconstitutional on separation of powers grounds because its "limitations on judicial review impose[] constitutionally impermissible restrictions on the judicial branch." Yahoo's Memorandum in Opposition to Motion to Compel (Yahoo's Mem. in Opp'n) at 21. In particular, Yahoo objects that, in proceedings under 50 U.S.C.A. § 1805c, judicial review is confined to the government's determination that its procedures are reasonably designed to ensure that acquisitions do not constitute "electronic surveillance," as defined at 50 U.S.C.A. §§ 1801(f) and 1805a, and that the FISC applies a "clear error" standard in reviewing that determination. Yahoo's Mem. in Opp'n at 21-22. Yahoo contends that these limitations are inconsistent with the scope and nature of the inquiry necessary for a court to determine, under prior judicial decisions, whether a surveillance[10] comports with the Fourth Amendment. Id. at 21-23. ~~(S)~~

As authority for its separation of powers objection, Yahoo cites Doe v. Gonzales, 500 F. Supp. 2d 379 (S.D.N.Y. 2007), which involved First Amendment challenges to non-disclosure obligations imposed on the recipient of a national security letter (NSL) under 18 U.S.C.A. § 2709 (West 2000 & Supp. 2007). In Doe, the separation of powers concerns derived from 18 U.S.C.A. § 3511(b) (West Supp. 2007), which governs the scope and standard of review to be applied by a district court when the recipient of an NSL petitions for relief from the non-disclosure obligations. 500 F. Supp. 2d at 409, 411-13.[11] Employing one of the quintessential tenets of separation of powers jurisprudence – that "Congress cannot legislate a constitutional standard of review that contradicts or supercedes what the courts have determined to be the standard applicable under the First Amendment for that purpose," Doe, 500 F. Supp. 2d at 411 (citing Dickerson v. United States, 530 U.S. 428, 437 (2000); Marbury v. Madison, 5 U.S. (1 Cranch) 137, 177 (1803)) – the Doe court invalidated certain aspects of § 3511(b).[12] ~~(S)~~

[redacted]

[11] The Doe court entertained facial challenges to sections 2709 and 3511 because those statutory provisions "are broadly written and certainly have the potential to suppress constitutionally protected speech." 500 F. Supp. 2d at 396. (U)

[12] See Doe, 500 F. Supp. 2d at 405-06 (under Freedman v. Maryland, 380 U.S. 51 (1965), government must bear burden of proving need for restriction on speech); id. at 409 (§ 3511(b)(2)'s limitations on judicial review of government's certification of need for non-disclosure was "plainly at odds with First Amendment jurisprudence which requires that courts strictly construe content-based restrictions and prior restraints to ensure they are narrowly (continued...)

Assuming arguendo that this separation of powers principle was correctly applied in Doe, it does not apply to the situation presented in this case. The limitations on judicial review legislated in § 1805c apply only to the ex parte review of the government's procedures submitted to the FISC under § 1805c(a). Here, the challenged event involves an effort by the Attorney General, under 50 U.S.C.A. § 1805b(g), to "invoke the aid of the [FISC] to compel compliance" with his directives. Under § 1805b(g), the FISC is to determine whether "the directive[s were] issued in accordance with [50 U.S.C.A. § 1805b(e)] and [are] otherwise lawful." The recipient of a directive, such as Yahoo, may raise Fourth Amendment challenges in response to a motion to compel compliance, see infra Part III.A, triggering an assessment by the FISC of whether acquisitions pursuant to the directive would violate the Fourth Amendment. The limitations on judicial review imposed on the separate, ex parte proceeding under § 1805c do not apply to the Court's analysis of Fourth Amendment issues in this case. Thus, the PAA does not intrude on the Court's "power to . . . decide what constitutional rule of law must apply" in this case. Doe, 500 F. Supp. 2d at 411. (S)

B. Yahoo's Other Non-Fourth Amendment Objections to the PAA Are Not Persuasive. (S)

Yahoo argues next that the PAA is "defective" or "problematic" in three other respects. Yahoo's Mem. in Opp'n at 23-24. First, it notes that 50 U.S.C.A. § 1805b(a)(1) and 50 U.S.C.A. § 1805c(b) use divergent language to describe the procedures to be adopted by the government and reviewed by the FISC, such that "it is unclear what should be submitted to, and reviewed by,

---

[12](...continued)
tailored to advance a compelling government interest"). (U)

this Court." Yahoo's Mem. in Opp'n at 23.[13] [redacted] Because this ambiguity can be resolved by such

---

[13] Compare § 1805b(a)(1) (requiring "reasonable procedures . . . for determining that the acquisition of foreign intelligence information . . . concerns persons reasonably believed to be located outside the United States" and providing that "such procedures will be subject to review" by the FISC under § 1805c) with § 1805c(b) (the FISC shall review for clear error "the Government's determination" that the § 1805b(a)(1) procedures "are reasonably designed to ensure that acquisitions . . . do not constitute electronic surveillance"). These procedures are separate from the "minimization procedures" required by § 1805b(a)(5). (U)

[14] In the context of the challenged directives here, the "tasked facilities" are those [redacted] identified by the government to Yahoo for acquisition. ~~(S)~~

[redacted]

(continued...)

interpretative analysis, there is no force to Yahoo's argument that it renders the challenged directives unlawful. (S)

Second, Yahoo raises a separate argument that challenges the propriety of enforcing the directives while judicial review of these procedures under 50 U.S.C.A. § 1805c(b) has not been

---

[redacted]

completed. Yahoo's Mem. in Opp'n at 23. A brief explanation of the procedures involved in this case will be useful before addressing the merits of this argument. ~~(S)~~

[redacted]

[redacted]

Yahoo claims that it "should not be required to comply with the Directives until this Court has approved the government's procedures" under 50 U.S.C.A. § 1805c(b). Yahoo's Mem. in Opp'n at 23. [redacted] (S)

[redacted] the Court finds that the terms of the PAA foreclose Yahoo's suggestion that the completion of judicial review under § 1805c(b) is a prerequisite to a directive's having compulsive effect. Upon the effective date of the PAA, see § PAA 6(a), the Attorney General and the Director of National Intelligence were empowered to authorize acquisitions of foreign intelligence information under § 1805b(a), and to issue directives "[w]ith respect to an authorization of an acquisition" under § 1805b(e). The recipient of a directive is obligated to "immediately provide the Government with all information, facilities, and assistance necessary to accomplish the acquisition." § 1805b(e)(1) (emphasis added). In contrast, Congress envisioned that judicial review of the government's procedures under § 1805c(b) could take up to 180 days after the effective date of the PAA to complete. See § 1805c(b). Congress plainly intended that directives could take effect before the § 1805c(b) process was completed.[19] Thus, Yahoo's second argument must also be rejected. (S)

Third, Yahoo challenges the directives, arguing that, under section 6(c)-(d) of the PAA, it remains obligated to comply with the directives for up to one year, even though the protection of immunity provided to it by the legislation may not apply by virtue of the lapse of 50 U.S.C.A. § 1805b(l). Yahoo's Mem. in Opp'n at 24. In response, the government asserts that the immunity provision remains in effect throughout the life of the directives. Memorandum in Support of Government's Motion to Compel (Mem. in Support of Gov't Motion) at 24 n.22. For essentially the same reasons that support the Court's holding that § 1805b(g) remains in effect with regard to the directives at issue by operation of § 6(d) of the PAA, see supra Part I, the Court finds that § 6(d) also preserves the operability of the immunity provision of § 1805b(l). Not only does § 1805b(l) fit comfortably within the preserving language of § 6(d), but it would be wholly illogical for Congress to have initially afforded civil immunity to the recipients of directives, only to have it subsequently extinguished even though the obligation to comply with the directives remains in effect.[20] (S)

---

[19] Yahoo's argument regarding the timing of judicial review under § 1805c(b) is also unpersuasive if construed as a Fourth Amendment challenge. As explained below, the Court finds that authorized acquisitions pursuant to the directives issued to Yahoo comport with the Fourth Amendment jurisprudence. See infra Part III.B-C. And, as part of the Court's assessment of compliance with the reasonableness requirement of the Fourth Amendment, the Court has reviewed the procedures in question, which seek to ensure that acquisitions will be directed at Yahoo accounts used by persons reasonably believed to be overseas. See infra note 83 and accompanying text. (S)

[20] Moreover, in Yahoo's case, any assistance rendered will be pursuant to this Court's

(continued...)

C. The PAA Does Not Require Certifications or Directives to Identify Each Individual Target. (S)

Yahoo also argues that the directives do not comply with the terms of the PAA, because they require Yahoo to assist in surveillance of persons who are not known to the government at the time of the certification, but rather become known to the government after the certification is made. Yahoo's Mem. in Opp'n at 24-25. Yahoo advances this argument despite its acknowledgment that 50 U.S.C.A. § 1805b(b) expressly states that a certification "is not required to identify the specific facilities, places, premises, or property at which the acquisition of foreign intelligence information will be directed." Yahoo opines that there is an implicit requirement that the government identify each <u>person</u> at whom the surveillance will be directed when a certification is made, and that the government can target persons identified thereafter only pursuant to a subsequent certification. Yahoo bases this argument on 50 U.S.C.A. § 1805b(a)(2), which requires the Attorney General and the Director of National Intelligence to issue a certification if they "determine, based on the information provided to them, that . . . the acquisition does not constitute electronic surveillance." Yahoo's Mem. in Opp'n at 24. Yahoo notes that 50 U.S.C.A. § 1805b(a)(1) separately requires the Attorney General and the Director of National Intelligence, before issuing a certification, to determine that "there are reasonable procedures in place for determining that the acquisition of foreign information . . . concerns

---

[20](...continued)
Order requiring compliance with the directives. And, failure to obey the Order "may be punished . . . as contempt of court." § 1805b(g). Under such circumstances, Yahoo would likely have recourse to some form of immunity, even apart from the express language of § 1805b(l). Cf. Rodriques v. Furtado, 950 F.2d 805, 814-16 (1st Cir. 1991) (qualified immunity for physician assisting in search authorized by warrant). (S)

persons reasonably believed to be located outside the United States." Yahoo's Mem. in Opp'n at 24-25. Yahoo argues that in order for § 1805b(a)(2) to have any independent effect, this provision must require the Attorney General and the Director of National Intelligence to determine, on an individualized basis, that each person at whom surveillance will be directed is outside of the United States, such that surveillance directed at them will not constitute "electronic surveillance" by virtue of 50 U.S.C.A. § 1805a. Yahoo's Mem. in Opp'n at 25. Otherwise, the argument continues, the determination under § 1805b(a)(2) would merely (and redundantly) rely on the efficacy of the procedures, which are already the subject of the determination under § 1805b(a)(1), in ensuring that new persons at whom the surveillance is later directed are outside of the United States. Yahoo's Mem. in Opp'n at 25. (S)

In response, the government essentially inverts Yahoo's argument by contending that, if § 1805b(a)(2) required individualized determinations by the Attorney General and the Director of National Intelligence regarding the location of each person at whom surveillance will be directed, then it would be superfluous for § 1805b(a)(1) to require procedures to ensure that the surveillance is directed at persons reasonably believed to be outside of the United States. Mem. in Support of Gov't Motion at 23. (S)

This appears to be another occasion where the PAA is not a model of clear and concise legislative drafting. See supra notes 13-15 and accompanying text. Nonetheless, for the reasons described below, the Court concludes that the government's interpretation of § 1805b(a)(1) and (a)(2) better serves the canon of statutory construction which requires that statutes be construed in a manner that promotes a "symmetrical and coherent regulatory scheme, and fit[s], if possible, all parts [of a statute] into an harmonious whole," such that the terms of the statute are "read in their context and with a view to their place in the overall statutory scheme." Food & Drug Admin. v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 133 (2000) (internal quotations and citations omitted). (U)

Under the PAA, both the Attorney General and the Director of National Intelligence must make determinations "in the form of a written certification, under oath, [and] supported as appropriate by affidavit" of Presidentially-appointed and Senate-confirmed national security officials or the head of an agency within the intelligence community. 50 U.S.C.A. § 1805b. However, in circumstances where "immediate action by the Government is required and time does not permit the preparation of a certification, . . . the determination of the Director of National Intelligence and the Attorney General shall be reduced to a certification as soon as possible but in no event more than 72 hours after the determination is made." Id. These requirements for senior executive branch official participation are generally comparable to the involvement required by 50 U.S.C.A. § 1804, when application is made to the FISC for an order authorizing electronic surveillance.[21] (U)

Requiring the executive branch to meet these procedural requirements every time it identifies a new person (or group of persons) at whom it intends to direct surveillance would substantially burden and very likely impede the intelligence gathering efforts authorized under

[21] See § 1804(a) (requiring approval of the Attorney General based upon his finding that the application satisfies applicable statutory criteria); § 1804(a)(7) (requiring certification by "the Assistant to the President for National Security Affairs" or a Presidentially-appointed, Senate-confirmed national security official). (U)

the PAA, compared to an interpretation that permits surveillance of newly-identified persons under a previously issued certification, assuming that the other requirements for conducting surveillance are satisfied. It is true that based on Yahoo's interpretation, surveillance of a newly-identified account could commence immediately if the user of the newly-identified account also used a separate account already covered by a prior certification. But, in many instances, it will not be self-evident whether that is the case, and the analytical effort devoted to this question would constitute an additional burden on intelligence agencies.[22] (S)

Imposing such burdens is contrary to the congressional intent of easing the procedural requirements for targeting persons reasonably believed to be outside of the United States, in order to allow intelligence agencies to pursue new overseas targets with greater expediency and effectiveness.[23] This objective is reflected in § 1805b(b)'s express statement that a certification need not "identify the specific facilities, places, premises, or property at which the acquisition of

[redacted]

[23] See 153 Cong. Rec. H9954 (daily ed. Aug. 4, 2007) (statement of Rep. Smith) (PAA "adopts flexible procedures to collect foreign intelligence from foreign terrorists overseas," and "does not impose unworkable, bureaucratic requirements that would burden the intelligence community"); see also 153 Cong. Rec. S10,869 (daily ed. Aug. 3, 2007) (statement of Sen. Bond) (PAA meets "the needs that were identified . . . to clear up the backlog because there is a huge backlog," resulting from "the tremendous amount of paperwork" involved in the pre-PAA FISA process). (U)

foreign intelligence information will be directed." In view of the evident purpose for enacting the PAA, the Court declines to find an implicit requirement that certifications specify the persons at whom surveillance will be directed. If Congress had intended a limitation of this magnitude on the flexibility it otherwise intended to confer when it passed into law the PAA, one would expect a much clearer statement of such intent. (U)

The Court therefore concludes that certifications and directives do not have to specify the persons at whom surveillance will be directed in order to comply with the PAA. This construction of the PAA -- wherein the Attorney General and the Director of National Intelligence determine that there are "reasonable procedures in place" regarding the overseas location of targeted persons under § 1805b(a)(1), the FISC reviews those procedures under § 1805c(b),[24] and intelligence agency personnel make reasonable assessments of the location of persons to be targeted in conformance with those procedures – provides a framework more conducive to the congressional purpose of enabling intelligence agencies to identify and pursue overseas targets with greater speed and efficacy. (U)

D. The Directives Issued to Yahoo Survive the Amendment of the Government's Certifications. ~~(S)~~

As explained above, see supra notes 3-4 and accompanying text, the government purported to amend each of the [redacted] certifications relevant to this proceeding prior to the

[24] The only judicial review that is necessarily mandated under the PAA is the FISC's review of these procedures under § 1805c(b); other modes of judicial review occur only in response to contingent decisions by parties, such as the government's decision to bring the instant motion to compel under § 1805b(g). The decision of Congress to single out the § 1805b(a)(1) procedures for mandatory judicial review suggests that Congress expected these procedures to be especially important in properly implementing the PAA. (U)

expiration of the PAA on February 16, 2008. The government contends that these amendments are effective, and that the government may use the directives that were issued to Yahoo prior to these amendments as the means for conducting acquisitions under the amended certifications. Government's Response to the Court's Order of February 29, 2008 (Govt.'s Resp. to Feb. 29 Order) at 6-12, 16-20. Yahoo, on the other hand, argues that the issuance of new directives is required to effectuate material amendments to certifications. Yahoo's Supp. Brief. on Stat. Issues at 6-12. ~~(S)~~

Now that the PAA has expired, it is by no means clear that the government could issue new directives at this time, or otherwise take additional steps to effectuate the changes it intended to implement by the amendments. See PAA § 6(c), (d). For this reason, the impact of the government's actions prior to the expiration of the PAA has assumed greater importance. (U)

1. Certifications May Be Amended and Such Amendments Do Not Necessarily Require the Issuance of New Directives. (U)

The PAA does not expressly address whether and how certifications may be amended, or what effect such amendments have on previously issued directives. Nevertheless, the following general principles can be gleaned from the text of the statute:

> (1) The Attorney General and the Director of National Intelligence must make a written certification in order to authorize acquisitions of foreign intelligence information under § 1805b(a).[25] (U)

---

[25] As noted earlier, in emergency situations, the Attorney General and the Director of National Intelligence may make the determinations in support of an acquisition less formally, and then make the written certification within 72 hours. § 1805b(a). This emergency provision does not apply to this case because the authorizations in question have at all relevant times been supported by written certifications. (U)

(2) Acquisitions may only be conducted in accordance with the applicable certification. § 1805b(d). (U)

(3) "With respect to an authorization of an acquisition," the Attorney General and the DNI may direct a person to provide assistance in the acquisition. § 1805b(e). (U)

These principles do not foreclose the possibility that the Attorney General and the Director of National Intelligence could amend previous certifications. Indeed, the government argues that the authority to make a certification logically implies the ability to modify a certification in response to changed circumstances, see Govt.'s Resp. to Feb. 29 Order at 8, a principle courts have recognized in other contexts.[26] [redacted] Yahoo, for its part, does not object to the general proposition that the government could amend certifications while the PAA was in effect. Yahoo's Supp. Brief. on Stat. Issues at 6. Accordingly, the Court concludes that, prior to the PAA's expiration, the Attorney General and the Director of National Intelligence were not categorically prohibited from amending certifications previously made under § 1805b. The more difficult issue, however, is whether an amendment to a certification required the issuance of a new (or appropriately amended) directive, or instead whether the previously issued directive was a proper and effective

[26] See, e.g., Belville Min. Co. v. United States, 999 F.2d 989, 997-98 (6th Cir. 1993) ("Even if an agency lacks express statutory authority to reconsider an earlier decision, an agency possesses inherent authority to reconsider administrative decisions, subject to certain limitations."); Gun South, Inc. v. Brady, 877 F.2d 858, 862-63 (11th Cir. 1989) (recognizing "an implied authority in . . . agencies to reconsider and rectify errors even though the applicable statute and regulations do not expressly provide for such reconsideration"). (U)

means to obtain assistance for acquisitions conducted in accordance with the post-amendment terms of the certification. To that issue the Court now turns.[27] (S)

[redacted]

[27] The government also argues that, on these questions of statutory interpretation, the Attorney General's and the Director of National Intelligence's decisions are entitled to deference under Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc., 467 U.S. 837 (1984). See Govt.'s Resp. to Feb. 29 Order at 8. Indeed, the government argues that an especially heightened version of Chevron deference is due in this case because the statute to be interpreted concerns foreign affairs. See id. (citing Springfield Indus. Corp. v. United States, 842 F.2d 1284, 1286 (Fed. Cir. 1988), and Population Inst. v. McPherson, 797 F.2d 1062, 1070 (D.C. Cir. 1986)). However, the government does not explain why, in this case, the conditions for according any level of Chevron deference are satisfied. See, e.g., Gonzales v. Oregon, 546 U.S. 243, 255-56 (2006) (Chevron deference applies only when agency interpretation of statute was promulgated pursuant to statutorily-delegated "authority to the agency . . . to make rules carrying the force of law") (internal quotations omitted). In any case, because the Court finds that the amended certifications are valid and may be effectuated through the previously-issued directives without according Chevron deference, it is unnecessary to decide whether Chevron applies to this case. (U)

[28] Congress used nearly identical language to describe third-party assistance under a PAA directive and under a FISC order to assist in an electronic surveillance authorized under § 1805.

(continued...)

[redacted]

[28](...continued)
See § 1805b(e)(1)-(3) (PAA directive); § 1805(b)(2)(B)-(D) (FISC order). (U)

[redacted] Under § 1805b(a), the certification made by the Attorney General and the Director of National Intelligence is the means of authorization required by the PAA in non-emergency situations, and must include certain determinations identified in § 1805b(a)(1)-(5). Acquisitions authorized by the Attorney General and the Director of National Intelligence under § 1805b must be conducted in accordance with the applicable certification (except under an emergency authorization, after which a written certification must be made within 72 hours under § 1805b(a)).[31] [redacted]

[29] In cases of emergency, the Attorney General may authorize electronic surveillance, provided that a FISC order approving such surveillance is obtained "as soon as practicable, but not more than 72 hours" after the Attorney General's authorization. § 1805(f). (U)

[30] See § 1805(c)(2)(A) (order "shall direct . . . that the minimization procedures be followed"); FISC Rule 10(c) (government must immediately inform FISC when "any authority granted by the Court has been implemented in a manner that did not comply with the Court's authorization"). The FISC's rules are available online at: <http://www.uscourts.gov/rules/FISC_Final_Rules_Feb_2006.pdf>. (U)

[31] The government suggests that there is also a non-emergency exception to this requirement, i.e., when the government has modified procedures that were originally adopted under § 1805b(a)(1) in response to an adverse ruling by the FISC under § 1805c(c), it may follow the new procedures even if that results in an acquisition that is not in accordance with the certification. See Govt.'s Resp. to Feb. 29 Order at 17. But those hypothetical circumstances are not presented here and the Court expresses no opinion on whether the government's view is correct. (U)

[redacted] So, too, the Attorney General and the Director of National Intelligence issue directives, pursuant to § 1805b(e), to compel third parties to assist in acquisitions that have been authorized under § 1805b(a). Directives may be issued only after the Attorney General and the Director of National Intelligence have made the determinations specified in § 1805b(a)(1)-(5) and, except in emergencies, those determinations must take the form of a written certification under § 1805b(a). (U)

[redacted] supports the conclusion that a certification may be amended without undermining the effectiveness of a previously issued directive, at least in some circumstances. Yahoo acknowledges that this is the case for "purely ministerial amendments." Yahoo's Supp. Brief. on Stat. Issues at 9 n.10. However, Yahoo contends that amendments that modify minimization procedures under § 1805b(a)(5) or "targeting" procedures under § 1805b(a)(1) are "material," Yahoo's Supp. Brief. on Stat. Issues at 8-9, and that materially amended certifications are tantamount to new certifications that require new directives. Id. at 9-10. [redacted]

Moreover, as a matter of logic, it does not follow that any material amendment to the terms of an authorization – whether they are embodied in a FISC order under § 1805 or an executive branch certification under § 1805b(a) – necessarily vitiates the obligation of third parties to assist in the authorized surveillance. The fact of an amendment does not imply that the pre-amendment authorization had been invalid. [redacted] Therefore, there is no reason why the amendment should necessarily extinguish a third party's obligation to assist the surveillance, [redacted] or a directive under § 1805b(e). And if that obligation is not extinguished, then there is no reason to require the government to issue and serve a new directive (or an amendment to the prior directive), provided that the prior directive still appropriately describes the obligations of the third party to assist surveillance conducted pursuant to the amended authorization.[32] (S)

2. Requiring the Government to Issue New Directives Would Not Appreciably Enhance Judicial Review of Directives Under the PAA. (S)

The Court has carefully considered whether, and to what extent, the issuance of new directives whenever a certification is materially amended would further the purposes of the PAA

---

[32] In addition, Yahoo's approach involves practical disadvantages. As the government correctly contends, see Govt.'s Resp. to Feb. 29 Order at 23, the issuance of multiple directives would involve at least a marginal increase in the risk of improper disclosure of classified information. (S)

by facilitating judicial review of directives in the context of government actions to enforce compliance under § 1805b(g), or challenges to directives brought by recipients under § 1805b(h). As explained below, the Court concludes that any such furtherance of congressional intent based on Yahoo's position is illusory, and accordingly provides no basis for construing the PAA to require the issuance of new or amended directives in all cases where there has been a material amendment of a certification. (S)

Yahoo makes three arguments regarding the availability of meaningful judicial review of directives. Yahoo's Supp. Brief. on Stat. Issues at 9-12. Although only the third of these arguments directly pertains to the impact of amendments, all three are considered below. (S)

The first argument contends that the PAA violates the Fourth Amendment because there is no mechanism for judicial review of the reasonableness of surveillance under § 1805b, unless and until a directive is challenged under § 1805b(h) or becomes the subject of an enforcement action under § 1805b(g). Yahoo's Supp. Brief. on Stat. Issues at 9-12. But the directives at issue in this case are the subject of such an enforcement action, and for reasons discussed below, see infra Part III.B-C, the Court determines that the requirements of the Fourth Amendment are satisfied. (S)

Secondly, Yahoo notes that the recipient of a directive does not have access to the underlying certification and procedures. Yahoo's Supp. Brief. on Stat. Issues at 10.[33] Yahoo

[33] The directives issued to Yahoo recite, in language tracking the terms of § 1805b(a)(1)-(5), that the Attorney General and the Director of National Intelligence have made the determinations required for them to authorize acquisition under the PAA, but Yahoo is correct that they do not provide any information about the basis for these determinations. See Feb. 2008
(continued...)

objects that this lack of access puts the recipient in the position of deciding whether to comply with the directive, and whether to seek judicial review, without the information necessary for a full assessment of the directive's lawfulness. Id. at 10-11. The Court appreciates this conundrum, but it has nothing to do with whether a second, post-amendment directive needs to be issued. Even in circumstances where there is no amendment, the recipient will not necessarily have access to the underlying certification and procedures. Indeed, the PAA specifically provides that, even when a recipient is a party to litigation involving the lawfulness of a directive under § 1805b(g) or (h), "the court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions of a submission, which may include classified information." § 1805b(k). With this provision, Congress created an opportunity for the government to provide a full record to the Court, without disclosing sensitive information to non-governmental parties.[34] Under other provisions of FISA, it is the norm for federal district courts

---

[33](...continued)
Classified Appendix at 30-31 (directive to Yaho[redacted] ~~(S)~~

[34] On February 20, 2008, the government filed a motion for leave, pursuant to § 1805b(k), to submit ex parte for the Court's in camera review a classified appendix containing a complete set of the certifications, amendments, and procedures pertaining to the directives to Yahoo. See Response to Ex Parte Order to Government and Motion for Leave to File Classified Appendix for the Court's Ex Parte and In Camera Review, filed Feb. 20, 2008. As referenced above, see supra note 3, Yahoo filed a motion for disclosure of that submission, as well as of the Memorandum Opinion and Order in In re DNI/AG Certifications. See Motion for Disclosure of Filings, filed Feb. 20, 2008. On February 28, 2008, the Court granted the government's motion and denied Yahoo's motion. See Order entered on Feb. 28, 2008. Under the circumstances of this case, the Court has been able to assess the lawfulness of the directives without the benefit of a more fully informed adversarial process. ~~(S)~~

to conduct an ex parte in camera review in assessing the basis for a prior authorization of surveillance.[35] (S)

If the recipient of a directive is not entitled to information about the basis for the underlying authorization, it follows logically that a rule requiring that any material amendment to a certification be supported by the issuance of new directives would not appreciably enhance the recipient's ability to litigate the lawfulness of a directive. Service of a new directive might put the recipient on notice that a certification has been amended, but it would not inform the recipient of the nature of the amendment. Thus, from the perspective of judicial review, the recipient would scarcely be better-equipped to contest the lawfulness of the underlying authorization by virtue of having received a second, post-amendment directive. (U)

---

[35] For example, under 50 U.S.C.A. § 1806(f), federal district courts have jurisdiction over challenges to the lawfulness of electronic surveillance conducted pursuant to FISC orders issued under § 1805. In such cases, the district court

> shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary proceeding would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.

§ 1806(f). After the filing of such an affidavit, materials may be disclosed to the aggrieved person "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." Id. "In practice, the government has filed an affidavit from the Attorney General in every case in which a defendant has sought to suppress FISA evidence," David S. Kris & J. Douglas Wilson, National Security Investigations and Prosecutions § 28:7 (2007), and "no court has ever ordered the disclosure to a defendant or the public of a FISA application or order." Id. § 29:3. Moreover, courts have found that such ex parte proceedings do not violate the constitutional rights of criminal defendants seeking to suppress the evidentiary use of FISA information. See, e.g., United States v. Belfield, 692 F.2d 141, 148 (D.C. Cir. 1982); United States v. Nicholson, 955 F. Supp. 588[redacted]a. 1997). (U)

Yahoo's third argument is that permitting the amendment of certifications without issuing new directives complicates judicial review by potentially presenting the FISC with a "moving target." Yahoo's Supp. Brief. on Stat. Issues at 11-12. It is true in this matter that the "target" has been displaced, and that the Court was only belatedly made aware of this fact. See supra notes 3-4 and accompanying text. And, the government now acknowledges:

> While litigation is pending before this Court regarding the legality of directives under the Protect America Act, the Government has an obligation to alert this Court to any material changes made to an authorization, an accompanying certification, or the procedures the Government uses in the course of its acquisition of foreign intelligence information. The Government's obligations to keep the Court informed of changes that may inform its analysis are amplified where as here the materials at issue are filed ex parte.

Govt.'s Resp. to Feb. 29 Order at 21. The Court agrees with this assessment, subject to the modification that, because they are so central to the case, the Court should be apprised immediately of any change to an authorization, certification, or set of procedures that pertains to a directive that is the subject of either (1) pending litigation under § 1805b(g) or (h); or (2) a FISC order compelling compliance with such directive. The Order accompanying this Opinion therefore directs the government to notify the Court forthwith of any such changes pertaining to the directives issued to Yahoo.[36] (S)

With these corrective measures in place, the "moving target" concern becomes manageable from the perspective of judicial review. Moreover, the alternative of requiring the government to issue new directives after a certification has been amended would not necessarily

---

[36] In issuing this requirement, the Court expresses no opinion on whether or to what extent the government now has the authority to make such changes, given the expiration of the PAA. (S)

simplify judicial review. Rather, the pending litigation regarding the lawfulness of the prior, superseded directives would presumably be mooted, therefore requiring the institution of a new challenge to the lawfulness of the new directives. This is hardly a desirable result from the Court's perspective. (S)

For these reasons, the Court concludes that the efficacy of judicial review would not be enhanced by requiring the government to issue new directives following a material amendment to a certification. (S)

3. The Particular Amendments in Question Do Not Require New Directives. (S)

Based on the foregoing analysis, <u>see</u> <u>supra</u> Part II.D.1-2, the Court concludes, as a general matter,[37] that the amendment of a certification does not require the issuance of a new (or amended) directive to replace a previously issued directive when the following conditions are present:

(1) The directive, when issued (<u>i.e.,</u> pre-amendment), was supported by a valid authorization;

(2) After the amendment, a valid (albeit modified) authorization remains in effect; and

(3) The previously issued directive accurately describes the obligations of the recipient regarding the assistance of acquisitions pursuant to the amended authorization. (S)

The Court now applies these criteria to the amendments at issue in this case. (U)

Prior to any amendments, the [redacted] certifications at issue contained each of the determinations specified in § 1805b(a)(1)-(5), and otherwise conformed with the requirements of

[37] With respect to amendments to procedures adopted under § 1805b(a)(1), the impact of the statutory timetable for submission to, and review by, the FISC under § 1805c(a) and (b) merits a separate evaluation. <u>See</u> <u>infra</u> Part II.D.4. (U)

the PAA. See Feb. 2008 Classified Appendix at [redacted] Moreover, each of the [redacted] Yahoo directives corresponded with its underlying certification, both in duration and in the nature of the information and assistance to be provided.[38] Therefore, as to all of the amendments, the first of the three above-stated conditions is satisfied. (~~S~~)

[redacted]

[redacted]

[redacted]

Accordingly, the Court finds that all three conditions are satisfied as to each of the amendments in this case. However, amendments to procedures under § 1805b(a)(1) also require consideration of the potential impact of the statutory timetable for the government to submit, and the FISC to review, such procedures under § 1805c(a) and (b). The Court's analysis of that issue follows. (~~S~~)

4. The Timetables for Submission and Review of Procedures Under § 1805c(a) and (b) Do Not Foreclose the Government from Amending Procedures Under § 1805b(a)(1). (U)

Section § 1805b(a)(1) requires "reasonable procedures . . . for determining that the acquisition of foreign intelligence information . . . concerns persons reasonably believed to be located outside of the United States," and these procedures are "subject to review of the [FISC] pursuant to" section 1805c. § 1805b(a)(1). The Attorney General was required to submit such procedures to the FISC "[n]o later than 120 days after the effective date" of the PAA. § 1805c(a). The FISC was required to complete its review of those procedures by "[n]o later than 180 days after the effective date" of the PAA. § 1805c(b). The statute expressly provides that those procedures "shall be updated and submitted to the Court on an annual basis." § 1805c(a). (U)

[redacted]

Presumably, the purpose of these annual submissions is for the Court to review the updated procedures under the standards provided by § 1805c(b) and (c), although no timetable for such Court review is statutorily provided.[41] (U)

The 120-day and 180-day timetables were followed with regard to the original [redacted] sets of procedures adopted under § 1805b(a)(1). See In re DNI/AG Certifications. The PAA does not expressly provide for the submission and review of procedures after these 120-day and 180-day intervals, but before an annual submission would become due. The government advances a construction of these provisions under which the 120-day and 180-day intervals would apply to the procedures initially adopted by the government, but would not preclude the government from adopting and submitting new or revised procedures at any time thereafter. Govt.'s Resp. to Feb. 29 Order at 23-28. The Court agrees that this construction is in accord with the purpose and structure of the PAA, because the alternative construction, under which the government could not submit new or revised procedures after 120 days, except as part of an "annual" update, would produce anomalous results. ~~(S)~~

Under the terms of § 1805b(a), the Attorney General and the Director of National Intelligence were empowered to authorize acquisitions while the PAA was in effect. To do so, they were required to make determinations, including a determination that the procedures adopted under § 1805b(a)(1) "will be subject to review of the [FISC] pursuant to [§ 1805c]." §

---

[41] However, when one takes into account that the PAA was originally enacted for a term of only 180 days (later extended to 195 days), see § 6(c), and that authorizations may be authorized "for periods up to one year," see § 1805b(a), the purpose of requiring submissions "on an annual basis" is less clear. (U)

1805b(a)(1). If the government could not submit procedures to the FISC for review after 120 days, then any authorizations after that time would necessarily have to rely on previously submitted procedures. But there is no apparent reason why Congress would have desired to prohibit the government from revising procedures, or adopting new ones, as warranted by new authorizations, or for that matter, other changed circumstances.[42] For example, previously submitted procedures might not be as well-suited for new authorizations, which could involve new classes of targets or new means of acquisition. Indeed, previously submitted procedures might not satisfy the requirements of § 1805b(a)(1) at all, when transplanted to the circumstances of a new authorization. In such a case, the inability to adopt new or revised procedures would prevent the Attorney General and the Director of National Intelligence from making the determination that is required by § 1805b(a)(1) in order to authorize otherwise valid acquisitions of foreign intelligence information. (U)

Yahoo, for its part, contends that the timing of the government's submission of procedures must not have the effect of avoiding judicial review under § 1805c. Yahoo's Supp. Brief. on Stat. Issues at 12-13. Indeed, judicial review of the procedures relevant to this case under § 1805c has not been avoided. FISC review under § 1805c of the § 1805b(a)(1) procedures adopted by the original, pre-amendment certifications has been completed. See In re DNI/AG Certifications. On the other hand, judicial review of the § 1805b(a)(1) procedures

[42] Indeed, Congress perceived a need to examine § 1805b(a)(1) procedures periodically, as evidenced by the requirement to update them annually under § 1805c(a). It would be inexplicable for Congress to have required annual review and updating, but to have prohibited such efforts on a more frequent basis when circumstances so required. (U)

adopted by the amended certifications has not been completed; however, the 180-day timetable for completion of the FISC review established by § 1805c(b) is properly subject to the same construction as the 120-day timetable for government submission of procedures established by § 1805c(a), i.e., that the 180-day timetable applies to the procedures initially submitted by the government. It is only natural to construe these parallel provisions in a similar matter. Thus, the Court concludes that the 180-day timetable applies to the completion of FISC review of procedures initially submitted by the government, and that the FISC may and should review procedures subsequently submitted by the government, even if such review cannot be completed within 180 days of the effective date of the PAA. ~~(S)~~

Moreover, the Court finds that, by virtue of § 6(d) of the PAA, the judicial review provisions of § 1805c remain operative with regard to the § 1805b(a)(1) procedures adopted under the amended certifications. The amendments adopting new § 1805b(a)(1) procedures were made on [redacted] see Feb. 2008 Classified Appendix at [redacted] while the PAA was still in effect. Those amendments modified authorizations under the PAA. Despite the subsequent lapse of the PAA, those authorizations "remain in effect until their expiration," and acquisitions made thereunder "shall be governed by the applicable provisions of . . . amendments" enacted by the PAA. PAA § 6(d).[43] The judicial review provisions of § 1805c were enacted by § 3 of the PAA and, by their terms, those provisions are "applicable" to the acquisitions conducted pursuant to the procedures in question. Thus, the Court finds that these procedures remain subject to judicial review under § 1805c. ~~(S)~~

---

[43] A more thorough analysis of § 6(d) is provided above. See supra Part I. (U)

For these reasons, the Court concludes that the government's amendments to the § 1805b(a)(1) procedures do not conflict with the judicial review provisions of § 1805c. ~~(S)~~

Accordingly, based on the analysis set out in this Part of the Opinion (Part II), the Court finds that (1) the directives issued to Yahoo comply with the PAA and – subject to the Court's analysis of Fourth Amendment issues, see infra Part III – remain in effect pursuant to the amended certifications; and (2) enforcement of the directives in this proceeding does not violate separation of powers principles. ~~(S)~~

III. The Directives to Yahoo Comply with the Fourth Amendment. (U)

A. Yahoo's Fourth Amendment Arguments Are Properly Before the Court. ~~(U)~~

Having disposed of most of Yahoo's arguments, the Court now turns to whether Yahoo can raise its claim that the directives at issue violate the Fourth Amendment rights of third parties. ~~(S)~~

In its memorandum in opposition to the government's motion to compel, Yahoo argued that implementation of the directives would violate the Fourth Amendment rights of United States citizens whose communications would be intercepted. The government filed a reply that not only responded to Yahoo's Fourth Amendment arguments on the merits, but also disputed Yahoo's right to raise them, since Yahoo was not claiming that its own Fourth Amendment rights would be violated if it complied with the directives. The Court then ordered further briefing on the issue of whether Yahoo's Fourth Amendment arguments were properly before the Court. For the reasons set forth below, the Court agrees with Yahoo that it can challenge the directives as violative of the Fourth Amendment rights of third parties. ~~(U)~~

The Court starts its analysis of this issue with three basic propositions. First, Yahoo's attempt to assert the Fourth Amendment rights of others as a defense to the government's motion to compel does not raise any Article III standing concerns. See Warth v. Seldin, 422 U.S. 490, 500 n.12 (1975) (a litigant's attempt to assert the rights of third parties defensively, as a bar to judgment against him, does not raise any Article III standing problem). Second, prudential standing rules frequently (though not always) prevent litigants from asserting the rights of third parties. See Kowalski v. Tesmer, 543 U.S. 125, 129 (2004) (a party generally must assert its own legal rights and interests, and cannot base its claim for relief on the legal rights or interests of third parties, but also noting exceptions to this rule); Warth, 422 U.S. at 500 n.12 (litigants who assert the rights of third parties defensively are also subject to prudential standing rules). Third, prudential limitations on standing do not apply where Congress has spoken and conferred standing to seek relief or raise defenses on the basis of the legal rights and interests of third parties. See Raines v. Byrd, 521 U.S. 811, 820 n.3 (1997); Warth, 422 U.S. at 501; Alderman v. United States, 394 U.S. 165, 174-75 (1969) (a Fourth Amendment case discussed further below). As to this third proposition, the Court concludes that Congress has indeed spoken here, and that Yahoo therefore may assert the Fourth Amendment rights of third parties as a defense to the government's motion to compel. (S)

The Court's analysis begins with the specific language of 50 U.S.C.A. § 1805b(g), which provides in pertinent part: "In the case of a failure to comply with a directive . . . . [t]he court shall issue an order requiring the person to comply with the directive if it finds that the directive was issued in accordance with subsection (e) and is otherwise lawful." Id. (emphasis added).[44] The plain reading of this language leads the Court to the conclusion that a government directive to Yahoo that violates the Fourth Amendment is not "otherwise lawful," regardless of whose Fourth Amendment rights are being violated.[45] (S)

Moreover, in the context of a statute that authorizes the government to acquire the contents of communications to and from United States persons[46] without their knowledge or consent, the protections provided by the Fourth Amendment are critically important. See, e.g., United States v. United States District Court, 407 U.S. 297 (1972); Katz v. United States, 389 U.S. 347 (1967). In this context especially, the expansive language that Congress used to

---

[44] Cf. 50 U.S.C.A. § 1805b(h)(2), which is a similar provision that would have applied if Yahoo had affirmatively filed a petition challenging the directive. Subsection (h)(2) provides, in pertinent part, that "[a] judge considering a petition to modify or set aside a directive may grant such petition only if the judge finds that such directive does not meet the requirements of this section or is otherwise unlawful." (emphasis added). (S)

[45] Indeed, the government implicitly acknowledged as much in its opening motion to compel, where, prior to any filing by Yahoo, the government argued that the directives in question were "otherwise lawful" precisely because they comported with any Fourth Amendments rights of third parties. Motion to Compel at 3-7. (S)

[46] Yahoo's arguments focus on the Fourth Amendment rights of United States citizens. The government, however, focuses on "United States persons," of whom United States citizens are a subset. Govt.'s Supp. Brief on the Fourth Amend. at 1, n.1. This Court agrees with the government's assertion that, "in general, the Fourth Amendment rights of non-citizen U.S. persons are substantially coextensive with the rights of U.S. citizens." Id. The phrase "United States person" is a term of art in the intelligence community that is defined in similar but not identical terms in FISA, 50 U.S.C.A. § 1801(i); Exec. Order No. 12,333, 3 C.F.R. 200 (1982), reprinted as amended in 50 U.S.C. § 401 (2000 & Supp. V 2005) (E.O. 12333); and the Department of Defense Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, DoD 5240.1-R (1982), Appendix A, definition 25. This Court will use the phrase "United States person" in referring to those persons who enjoy the protections of the Fourth Amendment. (S)

describe the Court's inquiry is difficult to reconcile with an intent to exclude the central question of whether compliance with a challenged directive would transgress the Fourth Amendment rights of United States persons whose communications would be acquired.[47] (U)

Despite the broad and unqualified nature of the statutory language (and notwithstanding what the government stated in its initial filing, see supra note 45), in subsequent filings the government is now urging the Court to conclude that Congress intended for the term "otherwise lawful" to preclude challenges to the legality of its directives based on the Fourth Amendment rights of third parties. See Mem. in Support of Gov't Motion at 5-7; Reply to Yahoo Inc.'s Sur-Reply. The government relies primarily on Supreme Court caselaw as support for its current position, in which the Court held that litigants could not raise the Fourth Amendment claims of others. The government also asserts that allowing Yahoo to raise the Fourth Amendment rights of others would lead to adjudication of those rights without sufficient concrete factual context.[48]

---

[47] The scant legislative history on the statutory provision at issue does not undermine its plain meaning. In the House, one proponent of the bill simply noted without further elaboration that, "[w]ith this new legislation . . . [t]he Court may also issue orders to assist the Government in obtaining compliance with lawful directives to provide assistance under the bill, and review challenges to the legality of such directives." See 153 Cong. Rec. H9965 (daily ed. Aug. 4, 2007) (statement of Rep. Wilson). In the Senate, one opponent of the bill charged that "[i]n effect, the only role for the court under this bill is as an enforcement agent – it is to rubberstamp the Attorney General's decisions and use its authority to order telephone companies to comply. The court would be stripped of its authority to serve as a check and to protect the privacy of people within the United States." See 153 Cong. Rec. S10,867 (daily ed. Aug. 3, 2007) (statement of Sen. Leahy). However, the remarks by an opponent of the legislation carry little weight. See United States v. Andrade, 135 F.3d 104, 108 (1st Cir. 1998). (U)

[48] The government cites South Dakota v. Opperman, 428 U.S. 364, 375 (1976) for this proposition, where the Supreme Court stated that, "as in all Fourth Amendment cases, we are obliged to look to all the facts and circumstances of this case." This Court is obviously obliged

(continued...)

However, these arguments do not persuade the Court to adopt the strained reading of the statutory language advocated by the government. (S)

The Court will assume, arguendo, that there is some validity to the government's argument that allowing Yahoo to assert the Fourth Amendment rights of third parties could be problematic because of inadequate factual context. But this is the type of prudential standing consideration that can be outweighed by countervailing considerations even in the absence of congressional action. See Kowalski v. Tesmer, 543 U.S. 125, 129-30 (2004) (discussing circumstances in which third parties may be granted standing to assert the rights of others). Here, however, Congress has spoken, and nothing absurd or outlandish will result from adhering to the natural meaning of its words. See generally Akio Kawashima v. Gonzales, 503 F.3d 997, 1000 (9th Cir. 2007) (plain meaning of statute controls absent an absurd or unreasonable result). The reality is that third parties whose communications are acquired pursuant to the government's directives will generally not be in a position to vindicate their own Fourth Amendment rights. It is unlikely that they will receive notice that the government is seeking or has already acquired their communications under the PAA unless the acquisitions are going to be used against them in an official proceeding within the United States, see 50 U.S.C.A. § 1805b(e)(1); 50 U.S.C.A. § 1806, and such proceedings will probably be rare given the foreign intelligence nature of the acquisitions and the fact that such acquisitions must concern persons reasonably believed to be outside the United States. See 50 U.S.C.A. § 1805b(a). Thus, allowing the recipient of a

---

[48](...continued)
to adhere to the directives of the Supreme Court, and will do so by examining all the facts and circumstances of this case, as reflected in the record before it, in rendering its decision. (U)

directive such as Yahoo to contest its constitutionality under the Fourth Amendment will generally be the only possible means to protect the Fourth Amendment rights of third parties, albeit on a relatively undeveloped factual record in some situations. Although Congress could have chosen a different path, the one reflected in the wording of the statute is far from absurd, and gives no cause to stray from the plain meaning of what Congress said. (S)

Furthermore, giving the "otherwise lawful" language its plain and obvious meaning is consistent with the Supreme Court precedent cited by the government concerning the assertion of Fourth Amendment rights. The government cites several cases, including Alderman v. United States, 394 U.S. 165 (1969), Rakas v. Illinois, 439 U.S. 128 (1978), and Minnesota v. Carter, 525 U.S. 83 (1998), in which the Supreme Court rejected attempts by criminal defendants to suppress evidence allegedly obtained in violation of others' Fourth Amendment rights. The government also cites a civil case, California Bankers Association v. Shultz, 416 U.S. 21 (1974), in which the Court stated that a bank could not challenge a provision of the Bank Secrecy Act on the grounds that the provision violated the Fourth Amendment rights of bank customers. None of these cases, however, support the government's position. (U)

In California Bankers, a bank, a bankers association, and individual bank customers challenged the Bank Secrecy Act of 1970, Pub.L. 91-508, 84 Stat. 1114, on Fourth Amendment grounds. In rejecting a challenge to the domestic reporting requirements of the Act and its implementing regulations, the Court held that the requirements did not violate the banks' own Fourth Amendment rights. California Bankers, 416 U.S. at 66. The Court also held that the depositor plaintiffs lacked standing to challenge the regulations, since they had failed to allege any transactions that would necessitate the filing of a report. Id. at 68. The Court then made the following statement without further explanation: "Nor do we think that the California Bankers Association or the Security National Bank can vicariously assert such Fourth Amendment claims on behalf of bank customers in general." Id. at 69. (U)

Although the unexplained nature of this last statement makes it difficult to know what the Court's rationale was for making it, one important point to note for purposes of this case is that there is no suggestion in the Supreme Court's opinion that the Bank Secrecy Act contained any language that even arguably conferred standing on a bank to assert the Fourth Amendment rights of its depositors. Thus, at most, California Bankers stands for the proposition that the banks in that case lacked prudential standing to assert the Fourth Amendment rights of their customers, in the absence of a congressional enactment affirmatively authorizing the banks to do so. See Haitian Refugee Center v. Gracey, 809 F.2d 794, 808-10 (D.C. Cir. 1987) (analyzing California Bankers as falling within the prudential standing rule that the plaintiff generally must assert his own legal rights and interests, while also noting that Congress may expressly confer third party standing so long as Article III is satisfied).[49] In the instant case, unlike California Bankers, Congress has enacted a provision that does appear to permit Yahoo to rely on the Fourth Amendment rights of others as a defense to a motion to compel. (TS)

[49] It is also possible that California Bankers was decided on a narrower ground entirely, i.e., that the plaintiff banks had failed to show that they had business with depositors whose transactions would require the filing of reports. See National Cottonseed Products Association, 825 F.2d 482, 491 n.11 (D.C. Cir. 1987) ("the Solicitor General's brief in California Bankers, however, suggested that depositors affected by the regulation in question were not so common as to make their business with the plaintiff banks predictable"). (U)

Turning now to the criminal cases cited by the government, in Alderman, the defendants were convicted prior to becoming aware that allegedly illegal electronic surveillance had been conducted. Alderman, 394 U.S. at 167. On appeal, they demanded a retrial if any of the evidence used to convict them was obtained in violation of the Fourth Amendment, regardless of whose Fourth Amendment rights had been violated. Id. at 171. The Court rejected that demand, and instead "adhere[d] . . . to the general rule that Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted." Id. at 174. The Court noted, however, that special circumstances that might justify expanded standing were not present. Id. And the Court specifically stated that "[o]f course, Congress or state legislatures may extend the exclusionary rule and provide that illegally seized evidence is inadmissible against anyone for any purpose." Id. at 175 (emphasis added). (U)

As Alderman demonstrates, it is perfectly consistent for the Supreme Court to hold that, in the absence of congressional action, Fourth Amendment rights (at least in the criminal suppression context) are "personal rights" that may not be asserted vicariously, while also envisioning that Congress might calibrate a different balance and confer expanded authority for third-party Fourth Amendment challenges as a matter of legislative prerogative. Thus, Alderman provides no support for a strained reading of the "otherwise lawful" legislative language. (U)

In Rakas, the Supreme Court reaffirmed the holding of Alderman that (at least in the criminal suppression context) Fourth Amendment rights are personal rights that cannot be vicariously asserted. Rakas, 439 U.S. at 133-34. The Rakas Court also determined that it served no useful analytical purpose to consider this principle as a matter of "standing." Thus, what had been analyzed as "standing" in Alderman and other earlier cases was now to be considered a substantive Fourth Amendment question, so that the suppression analysis would "forthrightly focus[] on the extent of a particular defendant's rights under the Fourth Amendment." Rakas, 439 U.S. at 139. (U)

This shift in analytical framework for criminal suppression motions does not support the government's position that Yahoo is barred from arguing that the directives to it are unlawful because they violate the Fourth Amendment rights of third parties. As the Court itself explained, its shift in Rakas from the rubric of "standing" to a pure "Fourth Amendment" analysis was not intended to affect the outcome of any cases. Id.[50] Furthermore, Rakas did not address a federal statute which affirmatively confers to a party the ability to assert another's Fourth Amendment rights, and nothing in Rakas undermined the statement in Alderman that Congress could "of course" confer what at the time was characterized as "standing" through legislative enactment.

[50] In this regard, the Court noted that "[r]igorous application of the principle that the rights secured by this Amendment are personal, in the place of a notion of 'standing,' will produce no additional situations in which evidence must be excluded. The inquiry under either approach is the same." Rakas, 439 U.S. at 139 (emphasis added); see also Rawlings v. Kentucky, 448 U.S. 98, 106 (1980). (U)

As this Court understands Rakas, the Supreme Court's "standing" analysis in Alderman and in other earlier cases, and the substantive analysis in Rakas itself, make clear that what had been called Fourth Amendment "standing" principles, properly applied, inexorably lead to the conclusion that a defendant in a criminal case seeking to suppress probative evidence on Fourth Amendment grounds could only assert his own Fourth Amendment rights, and not the Fourth Amendment rights of others. See Rakas, 439 U.S. at 132-39. It therefore made sense, in future cases, for courts to dispense with the "standing" nomenclature and proceed directly to the question of whether the defendant could make out a violation of his own Fourth Amendment rights. Rakas, 439 U.S. at 139. But as the Supreme Court made clear, no substantive change in the law was intended. (U)

Thus, nothing in Rakas requires this Court to read the "otherwise lawful" language in the manner suggested by the government. (S)

Finally, the government cites Minnesota v. Carter, 525 U.S. 83 (1998), a criminal suppression case in which the Supreme Court held that the Fourth Amendment rights of two criminal defendants were not violated by a police officer who looked through a drawn window blind into an apartment they were using to package cocaine. Id. at 85. There, the Supreme Court chastised the state courts in that case for using the discarded rubric of "standing,"[51] and reiterated that a criminal defendant seeking suppression had to demonstrate a violation of his own Fourth Amendment rights. Id. at 87-88. In analyzing whether the defendants' own Fourth Amendment rights had been violated, the Court stated that the text of the Fourth Amendment (which protects persons against unreasonable searches of "their" persons and houses) "indicates that the Fourth Amendment is a personal right that must be invoked by an individual." Id. at 88. Further, the Court noted, under Rakas, the individual seeking protection had to have a legitimate expectation of privacy in the invaded place. Id. The Court concluded that the defendants in that case had no legitimate expectation of privacy in the apartment they were temporarily using to package cocaine, and accordingly could not successfully challenge the seizure of the drugs. Id. at 89-91. (U)

Like Rakas, nothing in Carter suggests that this Court should read the congressional enactment at issue in a manner contrary to its most natural meaning. Rather, Carter merely

---

[51] The Carter Court stated that the shift in Rakas from standing to substantive Fourth Amendment law was "central" to the Court's analysis in Rakas. 525 U.S. at 88. This Court does not think, however, that this characterization of the analytical shift in Rakas undermines this Court's interpretation of Rakas, as set forth above. (U)

follows and applies Rakas, which precludes the assertion of another's rights in the absence of a federal statute authorizing one defendant to assert another defendant's Fourth Amendment rights. The language in those cases concerning the "personal" nature of Fourth Amendment rights echoes similar language in Alderman, but, as already noted, Alderman saw no inconsistency between such language and a congressional enactment that would extend the reach of the exclusionary rule. Furthermore, unlike the defendants in Carter, Yahoo is not "claim[ing] the protection of the Fourth Amendment," id. at 88; rather, Yahoo is claiming the protection of a federal statute that entitles it not to comply with an unlawful directive. Nothing in the text of the Fourth Amendment affirmatively precludes Congress from extending such protection to Yahoo, and Carter is not to the contrary. (S)

Finally, none of the courts of appeals cases cited by the government are apposite. In Ellwest Stereo Theatres, Inc. v. Wenner, 681 F.2d 1243, 1248 (9th Cir. 1982) (alternative holding), a movie arcade was deemed to lack standing to assert the Fourth Amendment rights of its customers. But, again, there is no hint of any legislative enactment that would have conferred upon the arcade the ability to make the challenge. Similarly, cases cited by the government that were brought under 42 U.S.C. § 1983 (2000) or Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics, 403 U.S. 388 (1971),[52] do not support the government's argument

---

[52] See Hollingsworth v. Hill, 110 F.3d 733, 738 (10th Cir. 1997) (Fourth Amendment rights are personal rights which may not be vicariously asserted in section 1983 action); Pleasant v. Lovell, 974 F.2d 1222, 1228-29 (10th Cir. 1992) ("To recover for a Fourth Amendment violation in a Bivens action plaintiffs must show that they personally had an expectation of privacy in the illegally seized items or the place illegally searched"); Shamaeizadeh v. Cunigan, 338 F.3d 535, 544-45 (6th Cir. 2003) (plaintiff in section 1983 action had no standing to assert (continued...)

in regards to the particular statute at issue here. The Court's holding in this situation is based on the specific wording of 50 U.S.C.A. § 1805b(g). And this language compels the conclusion that 50 U.S.C.A. § 1805b(g) confers upon Yahoo the ability to raise the Fourth Amendment rights of third parties whose rights would allegedly be violated if Yahoo complied with the directives issued to it, and that Yahoo's arguments on this score are properly before the Court. (S)

B. Yahoo's Fourth Amendment Arguments Fail on the Merits. (S)

The Court turns next to the merits of the Fourth Amendment issue. The crux of Yahoo's Fourth Amendment argument is that the directives are unconstitutional because they allow the government to acquire the communications of United States citizens without first obtaining a particularized warrant from a disinterested judicial officer. <u>See</u> Yahoo's Mem. in Opp'n at 10-13. Yahoo contends that there is no foreign intelligence exception to the Fourth Amendment's warrant requirement, but that even if such an exception exists, it does not apply to the directives issued to it under the PAA. <u>See</u> <u>id.</u> at 13-17. Finally, Yahoo asserts that even if a Fourth Amendment warrant is not required, the directives are still "unreasonable" under the Fourth Amendment. <u>See</u> <u>id.</u> at 19-21. (S)

The government counters by arguing that there is a foreign intelligence exception to the Warrant Clause of the Fourth Amendment, and that the exception is applicable to this case. <u>See</u> Mem. in Support of Gov't Motion at 8-12. The government further contends that surveillance of

---

[52](...continued)
the Fourth Amendment rights of his lessees); <u>but see</u> <u>Heartland Academy Community Church v. Waddle</u>, 427 F.3d 525, 532 (8th Cir. 2005) (cited by Yahoo) (statement that Fourth Amendment rights are personal and may not be vicariously asserted was made in context of exclusionary rule in criminal cases and is not controlling in a case under 42 U.S.C. § 1983). (S)

United States persons pursuant to the challenged directives is reasonable under the Fourth Amendment because the directives advance a compelling government interest; are limited in scope and duration; and are accompanied by substantial safeguards specifically designed to protect the privacy of United States persons. See id. at 13-20. (U)

The Court begins its analysis with the text of the Fourth Amendment, which provides:

> 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.

Yahoo contends[53] (and the government has not argued to the contrary) that "the people" protected by the Fourth Amendment include not only United States citizens located within the country's boundaries, but also United States citizens abroad as well, see United States v. Bin Laden, 126 F. Supp. 2d 264, 270-71 (S.D.N.Y. 2000) (Fourth Amendment protects American citizen in Kenya), and that the directives may sweep up communications to which a United States citizen is a party.[54] The Court assumes that United States citizens (and other United States persons, as well) will have a reasonable expectation of privacy in at least some of these communications, even though the scope of Fourth Amendment protection for email communications is not a settled

---

[53]See Yahoo's Mem. in Opp'n at 6-8. (S)

[54] In particular, Yahoo notes that its accounts with United States citizens reasonably believed to be abroad could be targeted directly under the directives, see Yahoo's Mem. in Opp'n at 7-8, and, in addition, communications between non-targeted United States citizens (who may be within the boundaries of the United States) and targeted accounts would also be acquired. See id. at 9. (S)

legal issue.[55] Indeed, the government has conceded the point.[56] Nevertheless, for the reasons stated below, the Court agrees with the government that the Fourth Amendment's Warrant Clause is inapplicable, because the government's acquisition of foreign intelligence under the PAA falls within the foreign intelligence exception to the warrant requirement.[57] ~~(S)~~

1. There is a Foreign Intelligence Exception to the Warrant Clause and It is Applicable Here. (U)

Yahoo correctly notes that the Supreme Court has never recognized a foreign intelligence exception to the warrant requirement. See United States v. United States District Court, 407 U.S. 297, 321-22 & n.20 (1972) (expressing no view as to whether warrantless electronic surveillance may be constitutional with respect to foreign powers or their agents, even as the Court held that there is no exception to the Fourth Amendment's warrant requirement for electronic surveillance conducted to protect national security against purely domestic threats). Nevertheless, the Court

---

[55] See David S. Kris & J. Douglas Wilson, National Security Investigations & Prosecutions at § 7:28. (U)

[56] See Govt.'s Supp. Brief on the Fourth Amend. at 2 ("U.S. Persons Abroad and U.S. Persons Communicating with Foreign Intelligence Targets Have a Reasonable Expectation of Privacy in the Content of Certain Communications Acquired Pursuant to the Directives") (emphasis in original); id. at 4 ([redacted] with respect to electronic communications of U.S. persons while [redacted] the Government does not contest that the acquisition contemplated by the directives would implicate the reasonable expectation of privacy of U.S. persons"). (U)

[57] This conclusion does not end the Court's Fourth Amendment inquiry, as the warrantless searches must also be "reasonable" upon consideration of all pertinent factors. See In re Sealed Case, 310 F.3d 717 (FISCR 2002) (discussed below); United States v. Bin Laden, 126 F. Supp. 2d at 277-82, 284-86 (conducting bifurcated Fourth Amendment inquiry into (1) whether the foreign intelligence exception to the warrant requirement was satisfied; and (2) whether the warrantless electronic surveillance at issue was reasonable). The Court resolves the reasonableness inquiry in the government's favor in Part III.B.2 of this Opinion. ~~(S)~~

is not without appellate guidance on this issue. In addition to being bound by decisions of the Supreme Court, the FISC must also adhere to decisions issued by the Foreign Intelligence Surveillance Court of Review (FISCR), the relationship of the FISC and the FISCR being akin to that of a federal district court and its circuit court of appeals. See, e.g., 50 U.S.C.A. § 1803(a) & (b); 50 U.S.C.A. § 1805b(i); cf. Springer v. Wal-Mart Associates' Group Health Plan, 908 F.2d 897, 900 n.1 (11th Cir. 1990) (district court bound by court of appeals precedent in its circuit). The FISCR has issued only one decision during its existence, but that decision bears directly on the existence of a foreign intelligence exception to the warrant requirement. (TS)

In In re Sealed Case, 310 F.3d 717 (FISCR 2002), the FISCR considered the constitutionality of electronic surveillance applications under FISA, as amended in 2001 by the USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001), but prior to enactment of the PAA. Under the individualized application procedure that was before the FISCR, the government submits an application for "electronic surveillance," as defined in 50 U.S.C.A. § 1801(f), to a FISC judge either prior to initiating surveillance or, under emergency procedures, shortly after such initiation. In order to approve such surveillance, the FISC judge must make a number of findings, including a probable cause finding that the target of the surveillance is a "foreign power" or an "agent of a foreign power," as defined in 50 U.S.C.A. § 1801(a) & (b). Furthermore, a high ranking executive branch official must certify, among other things, that "a significant purpose" of the surveillance is to obtain "foreign intelligence information," as defined in 50 U.S.C.A. § 1801(e). See generally 50 U.S.C.A. §§ 1801, 1803-1805. (U)

The FISCR held that the pre-PAA version of FISA was constitutional under the Fourth Amendment "because the surveillances it authorizes are reasonable." 310 F.3d at 746. In so holding, the FISCR expressly declined to decide whether an electronic surveillance order issued by a FISC judge constituted a "warrant" under the Fourth Amendment. In re Sealed Case, 310 F.3d at 741-42 ("a FISA order may not be a 'warrant' contemplated by the Fourth Amendment . . . . We do not decide the issue"); id. at 744 ("assuming *arguendo* that FISA orders are not Fourth Amendment warrants, the question becomes, are the searches constitutionally reasonable"). But if the Warrant Clause of the Fourth Amendment had been deemed applicable, it would have been necessary for the FISCR to decide whether a FISC electronic surveillance order under 50 U.S.C.A. § 1805 constituted a "warrant" under the Fourth Amendment. The FISCR did not feel compelled to decide that issue because it concluded that the President has inherent authority to conduct warrantless searches to obtain foreign intelligence information, so long as those searches are "reasonable" under the Fourth Amendment, noting:

> The *Truong* court,[[58]] as did all the other courts to have decided the issue, held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information. . . . We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President's constitutional power. The question before us is the reverse, does FISA amplify the President's power by providing a mechanism that at least approaches a classic warrant and which therefore supports the government's contention that FISA searches are constitutionally reasonable.

[58] United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980). (U)

In re Sealed Case, 310 F.3d at 742 (emphasis added). Thus, it is this Court's view that binding precedent requires recognition of a foreign intelligence exception to the Fourth Amendment's warrant requirement. (U)

The Court turns next to the contours of the exception. Caselaw indicates that two criteria must be satisfied in order for the foreign intelligence exception to the warrant requirement to apply. The first criterion, naturally, is that the government's actual purpose, or a sufficient portion thereof (and there is some dispute as to what degree is sufficient), be the acquisition of foreign intelligence. Second, a sufficiently authoritative official must find probable cause to believe that the target of the search or electronic surveillance is a foreign power or its agent. See United States v. Truong Dinh Hung, 629 F.2d at 915-16 (laying out criteria for the exception);[59] United States v. Bin Laden, 126 F. Supp. 2d at 277 (same); see also United States v. United States District Court, 407 U.S. at 321-22 (expressing no view on "the issues which may be

[59] In re Sealed Case was extremely critical of Truong's assessment that obtaining foreign intelligence must be the government's primary purpose in order to qualify for this exception from the warrant requirement. See infra pp. 61-62. However, there is nothing in In re Sealed Case that undermines or is otherwise inconsistent with the two criteria set forth in Truong and Bin Laden and applied herein. Certainly there is no suggestion in In re Sealed Case that there are additional criteria that need to be met before a court may conclude that the warrant exception is applicable and that a reasonableness analysis must therefore be undertaken. Furthermore, neither Yahoo nor the government has argued that there are some other, additional criteria that need be met for the foreign intelligence exception to apply. (S)

premise," and drawing a line that "was inherently unstable, unrealistic, and confusing." In re Sealed Case, 310 F.3d at 742-43 (emphasis in original). (U)

The FISCR having seemingly concluded that an electronic surveillance can fall within the foreign intelligence exception to the warrant requirement even if it merely has as a "significant purpose" the collection of foreign intelligence information, this Court rejects the proposition that the exception is inapplicable to acquisitions under the PAA because the pertinent officials are required to certify (and have certified in this case) merely that a "significant purpose" of an acquisition is to obtain foreign intelligence information. (U)

That brings the Court to the question of whether the acquisitions at issue satisfy the second prong of the foreign intelligence exception to the warrant requirement, which, as set forth above, would require a probable cause finding by an appropriate official that a United States person targeted for acquisition is a foreign power or an agent of a foreign power. Yahoo contends that this condition is not satisfied, because the PAA in fact authorizes surveillance directed at U.S. citizens abroad, whether or not they are agents of any foreign power. (S)

Yahoo's description of the PAA is correct. See 50 U.S.C.A. § 1805b. [redacted] The government maintains that this language requires the Attorney General to find probable cause that any U.S. person targeted under the certifications is a foreign power or an agent of a foreign power. See Mem. in Support of Gov't Motion at 12 n.10 & 15-16. ~~(S)~~

[redacted]

The Court agrees with the government that the language in the certifications concerning the applicability of the section 2.5 procedures is of significant importance. The issue before this Court is not what the PAA might authorize in the abstract; rather, the issue is the lawfulness of

---

[redacted]

the particular directives issued to Yahoo. The scope of each directive issued to Yahoo is determined and limited by the applicable certification. See 50 U.S.C.A. § 1805b(d) (an acquisition of foreign intelligence information under section 1805b may only be conducted in accordance with the certification by the DNI and AG, or in accordance with their oral instructions if time does not permit a certification). The Court therefore turns to the requirement in the certifications for Attorney General authorization pursuant to the section 2.5 procedures. ~~(S)~~

Section 2.5 of E.O. 12333 is a delegation to the Attorney General from the President to approve the use of certain techniques for intelligence collection purposes, "provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power." E.O. 12333, § 2.5.[64] As for "the procedures" under section 2.5 referenced in the certifications, the government's memorandum in support of its motion to compel identifies the Department of Defense Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, DoD 5240.1-R (1982) (DoD Procedures), as the applicable procedures. (U)

---

[64] Within the four corners of the Executive Order, section 2.5 specifically applies to the use for intelligence collection purposes "of any technique for which a warrant would be required if undertaken for law enforcement purposes." However, there is nothing in the certification language that incorporates this limitation. Rather, the fair import of the certification language is that Attorney General authorization is required for all acquisitions undertaken pursuant to these certifications that target a United States person abroad, and that the existing procedures for Attorney General authorization under section 2.5 shall be followed with regard to all such acquisitions. ~~(S)~~

Although the certifications could describe in clearer terms what is intended by their reference to "the procedures," the Court accepts the government's representation as to what is being referenced. The DoD Procedures by their terms apply to the NSA, which is a DoD intelligence component, see DoD Procedures, Appendix A, definition 8(a), and, as discussed below, individual procedures contained therein require Attorney General approval of proposed DoD intelligence activities in a manner consistent with section 2.5 of E.O. 12333. ~~(S)~~ [redacted]

In its memorandum in support of its motion to compel (filed prior to the submission of the amended certifications), the government cites specifically to Procedure 5, Part 2.C, which envisions, as a general rule,[65] that DoD intelligence components cannot direct "electronic

---

[redacted]

surveillance"[66] against a United States person who is physically outside of the United States for foreign intelligence or counterintelligence purposes unless the surveillance is approved by the Attorney General. Although it does not specifically use the term "agent of a foreign power," Procedure 5, Part 2.C provides what is tantamount to such a definition. Specifically, it requires that a request for Attorney General approval contain a statement of facts supporting a finding of probable cause that the target of the electronic surveillance is one of the following:

> (1) A person who, for or on behalf of a foreign power is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process), sabotage, or international terrorist activities, or activities in preparation for international terrorist activities; or who conspires with, or knowingly aids and abets a person engaging in such activities;
> (2) A person who is an officer or employee of a foreign power;
> (3) A person unlawfully acting for, or pursuant to the direction of, a foreign power. The mere fact that a person's activities may benefit or further the aims of a foreign power is not enough to bring that person under this subsection, absent evidence that the person is taking direction from, or acting in knowing concert with, the foreign power;
> (4) A corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or
> (5) A person in contact with, or acting in collaboration with, an intelligence or security service of a foreign power for the purpose of providing access to

---

[66] "Electronic surveillance" is defined under the DoD Procedures (Appendix A) as the

> [a]cquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication, or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction finding equipment solely to determine the location of a transmitter. (Electronic surveillance within the United States is subject to the definitions in the Foreign Intelligence Surveillance Act of 1978 (reference (b)).) (U)

information or material classified by the United States to which such person has access.[[67]]

In the context of the certifications at issue, the question becomes whether a finding of probable cause by the Attorney General that comports with Procedure 5, Part 2.C, is sufficient to invoke the foreign intelligence exception to the Warrant Clause. The Court finds that the answer is yes for the following reasons. (S)

First, the Attorney General is an appropriate official to make the probable cause finding. See United States v. Bin Laden, 126 F. Supp. 2d at 279 & n.18. Second, the descriptions in Procedure 5, Part 2.C, regarding what makes a United States person an acceptable target (i.e., an agent of a foreign power), themselves pass muster. Certainly in common sense terms, a United States person who falls into any of the five categories can reasonably be believed to be an "agent" of a foreign power.[68] Moreover, it also seems clear that categories 1, 3, and 5 suffer from no constitutional or other legal infirmities. See In re Sealed Case, 310 F.3d at 719 [redacted] target was an agent of a foreign power because there was probable cause that he or she was

---

[67] Procedure 7.C, which is applicable to physical searches, contains materially identical language as to a showing of probable cause concerning the target. (U)

[68] The Procedures independently define a "foreign power" as "[a]ny foreign government (regardless of whether recognized by the United States), foreign-based political party (or faction thereof), foreign military force, foreign-based terrorist group, or any organization composed, in major part, of any such entity or entities." DoD Procedures, Appendix A. [redacted] cf. 50 U.S.C.A. § 1801(a)(1) & (a)(4) (defining "foreign power" under FISA as including foreign governments, as well as groups engaged in international terrorism or activities in preparation for international terrorism). (S)

aiding, abetting, or conspiring with others in international terrorism); Bin Laden, 126 F. Supp. 2d at 278 (agent of al Qaeda). Similarly, to the extent the certifications contemplate targeting entities abroad as agents, the Court finds it unlikely that category four has any constitutional impediments either, at least not in the context of the foreign powers at issue (see supra note 68). Cf. 50 U.S.C.A. § 1801(a)(6) (even for purposes of a FISA order within the United States, the term "foreign power" includes an entity directed and controlled by a foreign government or governments). Finally, the second category admittedly does go beyond what FISA permits the government to do in the United States, cf. 50 U.S.C.A. § 1801(b)(1)(A) (limiting definition of "agent of foreign power" to a non-U.S. person acting in the U.S. as an officer or employee of a foreign power). Nonetheless, the Court concludes that it is constitutionally appropriate for the government to acquire for foreign intelligence purposes the communications of a United States person abroad who is acting as an officer or employee of [redacted] Indeed, were it otherwise, then the United States government would be routinely prevented from obtaining necessary foreign intelligence [redacted] Such a result would be untenable. ~~(S)~~

Based on the above analysis, the Court holds that the foreign intelligence exception to the warrant requirement is applicable to the directives issued to Yahoo. The Court must therefore address whether the directives are reasonable under the Fourth Amendment. ~~(S)~~

2. The Directives are Reasonable Under the Fourth Amendment (U)

The Fourth Amendment analysis merely begins with the finding that the government need not obtain a warrant to acquire the communications it seeks to obtain from Yahoo through the issuance of directives. In order for those directives to comport with the Fourth Amendment, they must also be reasonable. United States v. Knights, 534 U.S. 112, 118-19 (2001) ("The touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999))). And, to assess the reasonableness of the directives issued to Yahoo pursuant to the PAA, this Court must examine the totality of the facts and circumstances. Samson v. California, 547 U.S. 843, 848 (2006); Ohio v. Robinette, 519 U.S. 33, 39 (1996). ~~(S)~~

The acquisitions at issue in this case present this Court with the challenge of balancing the government's interest in acquiring foreign intelligence information against the privacy interests of those United States persons whose communications will be acquired.[69] There is little doubt about the weightiness of the government's interest, as this Court accepts the government's assertion that the information it seeks to acquire from Yahoo would "advance the government's compelling interest in obtaining foreign intelligence information to protect national security. . . ."

[69]The foreign intelligence that the government seeks to obtain from Yahoo is not limited to the communications of United States persons. Indeed, there is every reason to assume that most of the accounts that will be targeted will be ones used by non-United States persons overseas who do not enjoy the protections of the Fourth Amendment. See supra note 60. ~~(S)~~

Mem. in Support of Gov't Motion at 14; see also Gov't.'s Supp. Brief on the Fourth Amend. at 6 (". . . It is obvious and unarguable that no government interest is more compelling than the security of the Nation." (citing Haig v. Agee, 453 U.S. 280, 307 (1981))). ~~(S)~~

In furtherance of this objective, the government seeks to obtain from Yahoo communications that include communications to or from United States persons. See supra note 54. The directives at issue require Yahoo to provide to the government [redacted] information relating to targeted accounts, [redacted]

Declaration of [redacted] January 16, 2008; Declaration of [redacted] January 23, 2008 at 2 (noting, however, Yahoo's understanding that, at least initially, the government would only expect Yahoo to produce information [redacted]

[redacted]); Declaration of [redacted] January 23, 2008.[70] As noted above, the government concedes that at least some of this information is protected by the Fourth Amendment, and there is no question that extremely sensitive, personal information could be acquired through the directives, akin to electronic eavesdropping of telephone conversations. (~~T~~S)

Thus, unlike those circumstances involving a disparity between the importance of the government's interest and the degree of intrusiveness required to serve that interest, see, e.g., United States v. Martinez-Fuerte, 428 U.S. 543, 557-58 (1976) (analyzing traffic stops in which the government need is great but the intrusion is minimal), here there are weighty concerns on both sides of the equation. This Court, however, is not the first to assess the reasonableness of [redacted] Since the enactment of the Foreign Intelligence Surveillance Act, two particularly significant opinions have examined the Fourth Amendment reasonableness of the acquisition by the government of foreign intelligence information through the interception of communications of United States persons: the FISCR in In re Sealed Case, 310 F.3d 717 and the United States District Court for the Southern District of New York in United States v. Bin Laden, 126 F. Supp. 2d 264. (U)

---

[70] As may be obvious by the enumeration, this acquisition also will obtain [redacted] communications of those persons who send communications to or receive communications from targeted accounts, regardless of whether these communicants are located outside the United States and without regard to whether such individuals are agents of foreign powers. See infra Part III.B.2.e for a further discussion of these communications. (~~T~~S)

[71] [redacted] (U)

In determining the reasonableness of the acquisition at issue here, this Court will look to the factors considered by both courts, even though the facts of this case more closely resemble those presented in Bin Laden. However, because this Court is bound by the holding in In re Sealed Case, it must accord special consideration to that case in determining the extent to which the FISCR findings are applicable to a case such as this one, involving surveillance of United States persons abroad rather than within the boundaries of the United States. (U)

a. In re Sealed Case (U)

In re Sealed Case involved electronic surveillance conducted in the United States of the [redacted] communications of a United States person [redacted][72] As noted above, the FISCR implicitly found that the FISA orders fell within the parameters of the foreign intelligence exception to the warrant requirement. But, as this Court is also required to do, the FISCR closely examined various facts and circumstances to determine whether the issuance of those orders was reasonable under the Fourth Amendment. In re Sealed Case, 310 F.3d at 736-42. ~~(S)~~

The FISCR began its reasonableness analysis by looking to the requirements for the issuance of a warrant: issuance by a neutral detached magistrate, demonstration of probable

---

72 [redacted]

cause, and particularity. Id. at 738. The FISCR compared the procedural framework of the surveillance at issue in that case with the procedures required by the Omnibus Crime Control and Safe Streets Act of 1968, as amended, 18 U.S.C.A. § 2510 et seq. (West 2000 & Supp. 2007) (Title III)[73] and noted that to the extent a FISA order differed from a Title III order, "few of those differences have any constitutional relevance." Id. at 737. While it appears that the FISCR determined that the three factors recited above were the essential factors to consider in assessing the constitutionality (and hence, the reasonableness) of a FISA order, the FISCR also analyzed several other factors noting, "[t]here are other elements of Title III that at least some circuits have determined are constitutionally significant - that is, necessity, duration of surveillance, and minimization." Id. at 740 (citation omitted). The following factors all appear to have been considered by the FISCR in determining that the FISA orders were reasonable under the Fourth Amendment. (U)

i. Prior Judicial Review (U)

The FISCR assessed that Title III and FISA were virtually identical so far as the requirement for prior judicial approval. As such, the FISCR devoted little attention to analyzing this factor. However, given that the FISCR highlighted prior judicial review as one of the three essential requirements of the Fourth Amendment Warrant Clause, it seems apparent that the FISCR considered this to be a critical element in its reasonableness assessment. (U)

---

[73] "[I]n asking whether FISA procedures can be regarded as reasonable under the Fourth Amendment, we think it is instructive to compare those procedures and requirements with their Title III counterparts. Obviously, the closer those FISA procedures are to Title III procedures, the lesser are our constitutional concerns." In re Sealed Case, 310 F.3d at 737. (U)

ii. Probable Cause (U)

The FISCR noted that orders issued pursuant to FISA and Title III required different probable cause findings. Under FISA, the FISC need only find probable cause to believe "that the target is a foreign power or an agent of a foreign power," id. at 738 (citing 50 U.S.C.A. § 1805(a)(3)), while Title III requires "'probable cause for belief that an individual is committing, has committed, or is about to commit' a specified predicate offense," id. (quoting 18 U.S.C.A. § 2518(3)(a)). The FISCR acknowledged that while the FISA probable cause showing was not as great as that required under Title III, FISA incorporated "another safeguard not present in Title III," id. at 739 - a probable cause requirement, if the target is an agent, that "the target is acting 'for or on behalf of a foreign power'," id. The FISCR concluded that the import of this additional showing is that it would ensure that FISA surveillance was only authorized to address, "certain carefully delineated, and particularly serious, foreign threats to national security." Id. (U)

iii. Particularity (U)

In addressing particularity, the FISCR focused on two components: one concerning the nature of the communications to be obtained through the surveillance and the second concerning the relationship between the facilities to be targeted and the activity or person being investigated. Id. at 739-40. With regard to the former, FISA mandates that a senior executive branch official[74] certify the purpose of the surveillance, including the type of foreign intelligence information

[74]FISA identifies the officials authorized to make certifications as "the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate." 50 U.S.C.A. § 1804(a)(7). (U)

sought. 50 U.S.C.A. § 1804(a)(7). The FISC judge considering the application is obliged to grant such certification great deference. Id. at 739. Only when the target is a United States person does the FISC even make a substantive finding concerning that certification and even then, the standard of review is merely clear error. 50 U.S.C.A. § 1805(a)(5).[75] (U)

The findings made with regard to the facilities to be targeted are significantly different between the two statutes. Under FISA, the FISC must find probable cause to believe that the target is using or about to use the targeted facility, without regard to the purpose for which the facility will be used by the target. 50 U.S.C.A. § 1805(a)(3)(B); compare 18 U.S.C.A. § 2518(3)(d). As the FISCR noted, "[s]imply put, FISA requires less of a nexus between the facility and the pertinent communications than Title III, but more of a nexus between the target and the pertinent communications." Id. at 740. (U)

iv. Necessity (U)

The FISCR noted that while both statutes impose a necessity requirement, under FISA the assessment of necessity is made by the above-mentioned certifying official (a requirement not mandated by Title III), albeit subject to the above-described deferential standard of judicial review. Id. at 740. (U)

v. Duration (U)

Both statutes also address the length of time orders may remain in effect. FISA permits a longer duration than does Title III, but the FISCR found the difference between 30 days and 90

---

[75]Title III, on the other hand, requires that a judge make a probable cause finding that particular communications concerning the offense will be obtained. 310 F.3d at 739 (citing 18 U.S.C.A. § 2518(3)(b)). (U)

days to be reasonable in light of the "nature of national security surveillance, which is 'often long range and involves the interrelation of various sources and types of information.'" Id. (citations omitted). The FISCR took further comfort in the fact that "the longer surveillance period is balanced by continuing FISC oversight of minimization procedures during that period." Id. (U)

vi. Minimization (U)

Finally, in addressing the requirement for minimization that is embodied in both statutes, the FISCR acknowledged that Title III focuses on minimization at the time of acquisition (thus, more effectively protecting the privacy interests of non-target communications), while FISA permits minimization at both the acquisition and retention stages. Id. at 740. This discrepancy, according to the FISCR, "may well be justified[.] . . . Given the targets of FISA surveillance, it will often be the case that intercepted communications will be in code or a foreign language for which there is no contemporaneously available translator, and the activities of foreign agents will involve multiple actors and complex plots." Id. at 741.[76] (U)

In summary, the FISCR relied upon a variety of factors in finding the FISA statute constitutional, and thus, that orders issued pursuant to it were reasonable under the Fourth Amendment. While the FISCR appears to have placed great stock in the fact that FISA applications must be subjected to prior judicial scrutiny, the Court did not find it constitutionally problematic that a senior government official, rather than a detached magistrate, made findings

[76]The FISCR also addressed the amici filers' concerns that FISA does not parallel Title III's notice requirements or its requirement that a defendant may obtain the Title III application and order when challenging the legality of the surveillance. Id. at 741. The FISCR distinguished FISA from Title III in these two contexts and refused to find that the absence of these requirements undermined the reasonableness of the FISA orders under consideration. Id. (U)

comparable to those that Title III requires a judge to make. Id. at 739-41. The FISCR was also satisfied with the probable cause findings made under FISA, id. at 738-39, as well as with the extended duration of orders issued under it. Id. at 740. Both particularity requirements in FISA weighed into the FISCR's analysis and the FISCR did not negatively opine on the fact that one of those findings was made by a senior executive branch official rather than a judge. (U)

So, from the FISCR's opinion in In re Sealed Case, it is logical to assume that electronic surveillance targeted against United States persons [redacted] is reasonable under the Fourth Amendment under the following circumstances: (1) there is some degree of prior judicial scrutiny, (2) there is probable cause to believe that the target is an agent of a foreign power (or a foreign power itself), (3) there is probable cause to believe that the facility to be targeted is being used or is about to be used by the target, (4) at least some constitutionally required determinations are made by the senior executive branch officials designated in the statute, subject to a highly deferential degree of judicial review, (5) the duration may extend to 90 days, particularly when there is Court oversight over minimization procedures, and (6) such minimization procedures are in place and being applied. (S)

It is not clear from the FISCR opinion how much importance the Court attached to each of the above-described factors. For that reason, it is difficult to discern what effect the modification or removal of one of the factors would have on the overall determination of reasonableness. Nor is there clear guidance on how the requirements of reasonableness might vary for targets who are United States persons [redacted] (U)

b. United States v. Bin Laden (U)

A case that far more closely resembles the case now before this Court is United States v. Bin Laden, which involved search and surveillance targeted at a United States person located overseas. The facts there were the following. (U)

In its investigation of al Qaeda in Kenya, in August 1996, the intelligence community began monitoring telephone lines used by certain persons associated with al Qaeda, including Wadih El-Hage, an American citizen. Bin Laden, 126 F. Supp. 2d at 269. Although the government was aware that El-Hage was a United States person, it was not until eight months later, on April 4, 1997, that the Attorney General specifically authorized search and surveillance of El-Hage pursuant to E.O. 12333, § 2.5. Id. at 269 & n.23. (U)

At his criminal trial, El-Hage filed a motion to suppress evidence seized during the search of his home and the surveillance of his telephone and cellular telephone in Kenya, arguing that the search and surveillance violated his Fourth Amendment rights. Id. at 268, 270. The District Court found that the searches and surveillance conducted subsequent to the Attorney General's E.O. 12333 authorization fell under the foreign intelligence exception to the Fourth Amendment's warrant requirement and were reasonable; therefore, the evidence was lawfully acquired and not subject to suppression. Id. at 279, 288. However, the District Court found that surveillance conducted prior to April 4, 1997, was not incidental, as the government argued, and because the government had not obtained the Attorney General's authorization, was "not embraced by the foreign intelligence exception to the warrant requirement." Id. at 279. Further, because no warrant had issued, the Court found that the surveillance violated El-Hage's Fourth

Amendment rights. Id. at 281-82. However, for reasons not relevant to this matter, the Court declined to apply the exclusionary rule to the evidence that had been seized and intercepted. Id. at 282-84. (U)

As the District Court in Bin Laden noted, in order to find that the surveillance did not offend the Fourth Amendment, the Court needed to find not only that the government met the requirements of the foreign intelligence exception to the warrant requirement, but also that the conduct of the surveillance was reasonable. Id. at 284. There, the Court identified three factors as being essential in order to find that electronic surveillance targeted against a United States person abroad fit within the foreign intelligence exception to the warrant requirement: (1) the target must be an agent of a foreign power, (2) the primary purpose of the surveillance must be to acquire foreign intelligence, and (3) the President or the Attorney General must authorize the surveillance. Id. at 277.[77] The Bin Laden Court found that all three criteria were satisfied by virtue of the Attorney General's E.O. 12333 authorization. (U)

The District Court in Bin Laden then analyzed the reasonableness of the surveillance. Id. at 284-86. In response to El-Hage's concerns, the District Court acknowledged that the duration

[77]These criteria appear to derive directly from the holding in United States v. Truong, 629 F.2d 908 at 915. See Bin Laden, 126 F. Supp. 2d at 275, 277-79. As already noted, the FISCR took exception with Truong's articulation of the primary purpose requirement in its opinion in In re Sealed Case, 310 F.3d at 744. See supra pp. 61-62. Following the lead of the FISCR, as discussed above, this Court holds that the foreign intelligence exception to the warrant requirement requires only that a significant purpose of the acquisition is to obtain foreign intelligence information, there is probable cause to believe the individual who is targeted is an agent of a foreign power and that such probable cause finding is made by a sufficiently authoritative official, such as the Attorney General. (U)

of a surveillance may be a factor to consider in analyzing reasonableness. Id. at 286. However, the District Court accepted the government's argument that "more extensive monitoring and 'greater leeway' in minimization efforts are permitted in a case like this given the 'world-wide, covert and diffuse nature of the international terrorist group(s) targeted.'" Id. (citations omitted). As this quote suggests, the Court appears to have found that the existence of minimization procedures bears upon reasonableness, although the Court did not address the necessary parameters of such procedures. Id. Finally, as part of its reasonableness analysis, the District Court, citing United States v. Scott, 516 F.2d 751, 759 (D.C. Cir. 1975), found it significant that the telephones were used communally by al Qaeda agents, thereby making it more reasonable for the government to monitor them than it would be if the phones were primarily used for legitimate, non-foreign intelligence-related purposes. Id. (U)

Thus, the factors the Bin Laden Court appears to have relied upon to assess the reasonableness of the surveillance were: (1) the existence of minimization procedures, (2) the duration of the monitoring as balanced against both the minimization procedures and the nature of the threat being investigated, and (3) the extent to which the targeted facilities are used in support of the activity being investigated. (U)

c. Reasonableness Factors (U)

i. Common Factors Utilized in Both In re Sealed Case and Bin Laden

Comparing the factors relied upon by the FISCR in In re Sealed Case and by the District Court in Bin Laden, some factors are common in both cases. These factors can provide the starting point for this Court's reasonableness analysis of the directives issued to Yahoo. Both courts favorably noted that probable cause findings were made with regard to the target being an agent of a foreign power, In re Sealed Case, 310 F.3d at 738; Bin Laden, 126 F. Supp. 2d at 277-78, with the District Court expressly finding this factor to be an essential criterion for meeting the requirements of the foreign intelligence exception to the warrant requirement, id. at 277. Both Courts also relied upon the existence of minimization procedures in finding the surveillance at issue reasonable. In re Sealed Case, 310 F.3d at 740-41; Bin Laden, 126 F. Supp. 2d at 286. In addition, both Courts examined the duration of the authorized surveillance and both intimated that a longer duration must be balanced by more rigorous minimization procedures than might be reasonable for a shorter period of surveillance. In re Sealed Case, 310 F.3d at 740; Bin Laden, 126 F. Supp. 2d at 285-86. On this point, the FISCR found a 90-day duration reasonable and the District Court seemed to find a several month duration to be reasonable (although it is not clear whether the District Court predicated its assessment on the 90-day re-authorization by the Attorney General in July 1997). Id.[78] Both Courts found it reasonable that at least some findings were made by high level executive branch officials, even though not made by a judge. In re Sealed Case, 310 F.3d at 739-40; Bin Laden, 126 F. Supp. 2d at 279. The District Court specifically found it necessary that the Attorney General or the President make the probable cause findings, id. at 279, while the FISCR was satisfied that other senior executive branch officials make at least some of the necessary findings. In re Sealed Case, 310 F.3d at 739. The

---

[78]The District Court seemed to accept the defendant's assertion that the surveillance against him had continued for many months. Bin Laden, 126 F. Supp. 2d at 285-86. It is unclear from the District Court opinion the significance it attached to the fact that the Attorney General, in accordance with E.O. 12333, re-authorized the surveillance 90 days after her initial authorization. Id. at 279. (U)

FISCR explicitly relied upon the fact that there was a finding as to the facilities being targeted, distinct from and in addition to the finding that the targeted individual is an agent of a foreign power. Id. at 739-40. The District Court, while it did not directly hold that there is a requirement for a prior finding concerning the targeted facilities, favorably noted that it was "highly relevant" that the targeted telephones were "'communal' phones which were regularly used by al Qaeda associates." Bin Laden, 126 F. Supp. 2d at 286. ~~(S)~~

ii. Factors Weighed Differently by the Two Courts (U)

Two of the factors considered by the courts appear to have been weighed differently. The District Court explicitly rejected the requirement of prior judicial review of the government's application, id. at 275-77, while the FISCR found this to be an important consideration, In re Sealed Case, 310 F.3d at 738. And, while the FISCR explicitly addressed the requirement that there be a prior finding of probable cause to believe that a particular facility is being or will be used by the targeted agent, id. at 739-40, the District Court referred to this consideration only peripherally, Bin Laden, 126 F. Supp. 2d at 286. (U)

* Prior Judicial Review Not Required (U)

The FISCR favorably noticed that FISA orders are subject to prior judicial approval. The District Court, on the other hand, determined that such approval was not necessary under the circumstances of the case before it. [redacted] ~~(S)~~

Without question, Congress is aware, and has been for quite some time, that the intelligence community conducts electronic surveillance of United States persons abroad without seeking prior judicial authorization. In fact, when Congress enacted FISA in 1978, it explicitly excluded overseas surveillance from the statute, as reflected in a House of Representatives Report that states, "this bill does not afford protections to U.S. persons who are abroad . . ." H.R. Rep. No. 95-1283, pt. 1 at 51 (1978). See also Bin Laden, 126 F.Supp. 2d at 272 n.8 (noting that FISA only governs foreign intelligence searches conducted within the United States). The Bin Laden Court examined the issue of prior judicial approval in the same context presented to the Court in this case, and observed that "[w]arrantless foreign intelligence collection has been an established practice of the Executive Branch for decades." Id. at 273 (citation omitted). Citing Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 610 (1952) ("[A] systematic, unbroken, executive practice, long pursued to the knowledge of Congress and never before questioned, engaged in by Presidents who have also sworn to uphold the Constitution, making as it were such exercise of power part of the structure of our government, may be treated as a gloss on 'Executive Power' vested in the President by § 1 of Art. II.") and Payton v. New York, 445 U.S. 573, 600 (1980) ("A longstanding, widespread practice is not immune from constitutional scrutiny. But neither is it to be lightly brushed aside."), the District Court further noted that, "[w]hile the fact of [congressional and Supreme Court silence with regard to foreign intelligence collection abroad] is not dispositive of the question before this Court, it is by no means insignificant." Bin Laden, 126 F. Supp. 2d at 273. This Court finds the reasoning of the District Court persuasive and therefore accepts as a general principle, that prior judicial approval of an acquisition of foreign intelligence information targeted against a United States person abroad is not an essential element for a finding of reasonableness under the Fourth Amendment. (U)

* Probable Cause to Believe that the Targeted Facility is Being or is About to be Used (U)

The FISCR directly, and favorably, addressed the requirement in FISA that a prior showing be made that the targeted individuals were using or were about to use the targeted facilities. In re Sealed Case, 310 F.3d at 739-40. The District Court considered this factor more obliquely. Bin Laden, 126 F. Supp. 2d at 286. (U)

The FISCR characterized the judicial finding of probable cause to believe the targeted facility is being or is about to be used by the targeted agent as a particularity requirement, and therefore, one of the required elements of a Fourth Amendment warrant. Given that the FISCR analyzed reasonableness in relation to the warrant requirement, it is not surprising that the FISCR found this factor to be constitutionally significant in assessing reasonableness. In re Sealed Case, 310 F.3d at 739-40. The District Court in Bin Laden expressed no direct view on this factor, nor does its opinion make clear if the Attorney General's authorizations included a probable cause finding regarding the use of the facilities to be targeted. However, as noted above, the District Court did consider the use of the targeted facilities in its reasonableness assessment. Bin Laden, 126 F. Supp. 2d at 286. [redacted] The Fourth Amendment particularity requirement serves, in large part, as a check to minimize the likelihood that persons who have a reasonable expectation of privacy are not mistakenly subjected to government surveillance.[79] When the surveillance activity is conducted against persons outside the United States, the persons who would be inappropriately surveilled most likely would be non-United States persons. And, this is not a class of persons who enjoy the protections of the Fourth Amendment. Therefore, it seems reasonable that, in the overseas context, there is less of a need to require a prior showing of probable cause to believe that a properly targeted individual is using or is about to use a specific, targeted facility. ~~(S)~~

iii. Necessity (U)

The FISCR noted that FISA incorporates a "necessity" provision, as does Title III. In re Sealed Case, 310 F.3d at 740. The District Court in Bin Laden, however, makes no mention of necessity. A showing of necessity is not always a prerequisite for reasonableness. Illinois v. Lafayette, 462 U.S. 640, 647 (1983) ("[t]he reasonableness of any particular governmental activity does not necessarily or invariably turn on the existence of alternative 'less intrusive' means"). And, this Court is not persuaded that, in the context of the PAA, any ameliorative purpose would be served by requiring the government to demonstrate that less intrusive means have been attempted. Indeed, the very purpose of the PAA is to provide the government with "flexible procedures to collect foreign intelligence from foreign terrorists overseas . . . [that do]

---

[79]While discussions of the particularity requirement typically focus on the "property to be sought" rather than the person using that property, Berger v. New York, 388 U.S. 41, 59 (1967), it is clearly the privacy interests of the individual that the Constitution protects. Verdugo-Urquidez, 494 U.S. at 266. Thus, in the context of electronic surveillance of email communications, if the government surveils the wrong email account, the harm would be against the privacy interests of persons whose communications were improperly acquired. (U)

not impose unworkable, bureaucratic requirements that would burden the intelligence community." 153 Cong. Rec. H9954 (daily ed. Aug. 4, 2007) (statement of Rep. Smith). Therefore, this Court will not consider the availability of less intrusive means as a factor in determining the reasonableness of the directives issued to Yahoo. ~~(S)~~

iv. Warrant Exception Criteria Are Factors to Consider in Assessing Reasonableness. (U)

The factors that provide the basis for the foreign intelligence exception to the warrant requirement (a significant foreign intelligence purpose and probable cause to believe that any United States person who is targeted is an agent of a foreign power) are also key elements that weigh in assessing reasonableness. (U)

d. Application of the Reasonableness Factors to the Acquisition of Targeted United States Persons' Communications Through the Directives Issued to Yahoo ~~(S)~~

In assessing the Fourth Amendment reasonableness of the acquisition of foreign intelligence information through the directives issued to Yahoo, this Court relies on the findings made above in Part III.B.1 of this Opinion, in which it found that the surveillance satisfies the requirements for the foreign intelligence exception to the warrant requirement. In addition, this Court will consider the following factors relied upon by the FISCR in <u>In re Sealed Case</u> and the District Court in <u>Bin Laden</u>: (1) minimization, (2) duration, (3) authorization by a senior government official, and (4) identification of facilities to be targeted. ~~(S)~~

But, first, this Court must acknowledge the statutory framework that governs the proposed acquisitions. The PAA only authorizes "the acquisition of foreign intelligence information <u>concerning persons reasonably believed to be outside the United States ...</u>" 50

U.S.C.A. § 1805b(a) (emphasis added). The statute further requires that "there are reasonable procedures in place for determining that the acquisition of foreign intelligence 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 105C of this Act." 50 U.S.C.A. § 1805b(a)(1) (emphasis added).[80] (U)

This Court sees no reason to question the presumption that the vast majority of persons who are located overseas are not United States persons and that most of their communications are with other, non-United States persons,[81] who also are located overseas. Thus, most of the communications that will be obtained through the directives issued to Yahoo likely will be communications between non-United States persons abroad, i.e., persons who do not enjoy the protection of the Fourth Amendment.[82] So, to the extent "reasonable" procedures represent an effort to minimize the likelihood of targeting the wrong facility or the wrong person or of obtaining the communications of non-targeted communicants, a program such as this, which is focused on overseas collection, presents fewer Fourth Amendment concerns than does a program

---

[80]See supra Part II.B for this Court's resolution of the ambiguities related to this provision. (U)

[81]This common sense presumption is embodied in the Department of Defense procedures governing the collection of information about United States persons, which state, "[a] person known to be currently outside the United States, or whose location is not known, will not be treated as a United States person unless the nature of the person's communications or other available information concerning the person give rise to a reasonable belief that such person is a United States citizen or permanent resident alien." DoD Procedures, Procedure 5, Part 3.B.4. (U)

[82]Supra note 69. (U)

that focuses on domestic communications within the United States.[83] It is against this backdrop that this Court will assess the appropriate reasonableness factors. (~~S~~)

i. Minimization (U)

By statute, the communications that will be acquired through the directives issued to Yahoo will be subject to minimization procedures that are supposed to comport with the definition of "minimization procedures" under 50 U.S.C.A. § 1801(h). 50 U.S.C.A. § 1805b(a)(5). This Court has reviewed the minimization procedures applicable to these directives and finds that they are virtually the same procedures the government uses for many non-PAA FISA collections. Feb. 2008 Classified Appendix at [redacted] In other contexts, this Judge has (as other Judges on the FISC have) found these non-PAA procedures to be reasonable under circumstances in which the government is intercepting private email communications. (~~S~~)

This Court, therefore, finds the minimization procedures filed by the government to be sufficiently robust to protect the interests of United States persons whose communications might be acquired through the acquisition of information obtained through the directives issued to

---

[83]This Court appreciates Yahoo's concern that "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." Yahoo's Mem. in Opp'n at 9. However, the Court has reviewed the government's targeting procedures and notes that the government has specifically addressed this issue and has robust procedures in place to [redacted] cease such surveillance "without delay[]" when it is determined that the target is in the United States. Feb. 2008 Classified Appendix at [redacted] see also id. at [redacted] (~~S~~)

that the 90-day duration was reasonable in part because the FISC exercised oversight over the minimization procedures while a surveillance is being conducted. Id. But, the PAA does not provide a similar role for the FISC. Notably, though, under the PAA, the target of the surveillance will be located overseas, and presumably, so will be a significant number of the persons who communicate with that target, while under a domestic FISA surveillance, it is feasible, and indeed likely, that the bulk of the information obtained would be to, from, or about United States persons. Therefore, to the extent judicial oversight over minimization serves to enhance the protection afforded United States persons whose communications are intercepted, the importance of such oversight wanes when a reduced proportion of United States person information will be acquired. Indeed, in Bin Laden, there was no judicial oversight of the minimization procedures whatsoever. And, in that case, the Court did not find a duration of approximately eight months to be unreasonable.[85] Therefore, on balance, this Court finds a 90-day duration for the acquisition of communications targeting United States persons under the circumstances presented in this case, even without judicial oversight of the application of the minimization procedures, reasonably limited. (U)

iii. Senior Official Approval (U)

Prior to the issuance of its directives to Yahoo, as required by the statute, the Attorney General and the Director of National Intelligence determined, through written certifications under

[85] Supra note 78 and accompanying text. (U)

oath, that were supported by affidavits from the Director of NSA, that

> there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under section 105B . . . concerns persons reasonably believed to be located outside the United States[,] . . . the acquisition does not constitute electronic surveillance as defined in section 101(f) of the Act[,] the acquisition involves obtaining foreign intelligence information from or with the assistance of communications service providers . . .[,] a significant purpose of the acquisition is to obtain foreign intelligence information and [,] the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section 101(h) of the Act.

Feb. 2008 Classified Appendix at [redacted] see also id. at [redacted]

[redacted] It is this Court's view that the certifications of these two officials represent a sufficient restraint on the exercise of arbitrary action by those in the executive branch who are effecting the actual acquisition of information, see In re Sealed Case, 310 F.3d at 739 (characterizing congressional intent that the certification by senior officials, "typically the FBI Director [with approval by] the Attorney General or the Attorney General's Deputy," would provide written accountability and serve as "an internal check on Executive Branch arbitrariness") (citation omitted); H.R. Rep. 1283 at 80, and thus weighs favorably in assessing the reasonableness of the directives issued to Yahoo. ~~(S)~~

iv. Identifying Targeted Facilities (U)

The final factor to consider in determining the reasonableness of the directives is the identification of the accounts to be targeted. As discussed above, the manner in which accounts are targeted for surveillance is an important consideration in determining the reasonableness of a warrantless surveillance.[86] For the following reasons, the Court finds that the current procedures employed by the government are reasonable, given all the facts and circumstances of the anticipated acquisition. (U)

In a typical foreign intelligence case where the intelligence activity is conducted within the United States, the government first establishes probable cause to believe that a particular individual is an agent of a foreign power and then identifies the specific facility the person is using that the government wants to monitor. By establishing probable cause to believe that the target is using a particular facility (as is required under the non-PAA provisions of FISA, 50 U.S.C.A. §§ 1804(a)(3)(B) & 1805(a)(3)(B)), the government is demonstrating the nexus between the person being targeted and the facility that is going to be monitored. This nexus requirement diminishes the likelihood that the government will monitor the communications of a completely innocent United States person, which would, on its face, appear to be an unreasonable search, and thus, violative of the Fourth Amendment. (U)

The PAA, by its terms, however, only allows the acquisition of communications which are reasonably believed to be used by persons <u>located outside the United States</u>. 50 U.S.C.A. §§ 1805a & 1805b(a). As stated above,[87] this Court can envision no reason to question the presumption that most people who are located outside the United States are not United States

---

[86]The Court is mindful that the PAA specifically provides that "[a] certification under subsection (a) 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.A. § 1805b(b); <u>see also</u> <u>supra</u> Part II.C. (U)

[87]<u>Supra</u> note 81. (U)

persons. So, even if, after establishing probable cause to believe a particular United States person is an agent of a foreign power, the government, pursuant to the PAA, mistakenly targets an account used by someone other than that United States person, the likelihood is that the person whose privacy interests are implicated is a person who does not enjoy the protection of the Fourth Amendment. (U)

[redacted]

v. In Sum, the Acquisition of Foreign Intelligence Information Targeting United States Persons Abroad Obtained Pursuant to the Directives Issued to Yahoo is Reasonable Under the Fourth Amendment. (S)

Having considered the totality of the facts and circumstances, including:

(1) the statute, which by its terms, limits acquisition to foreign intelligence communications of persons reasonably believed to be located outside the United States and requires written procedures for establishing the basis for making these determinations, procedures that have been reviewed by the Court;

(2) United States persons will not be targeted unless the Attorney General has determined, in accordance with E.O. 12333, § 2.5 procedures, that there is probable cause to believe that such person is an agent of a foreign power;

(3) the Director of National Intelligence and the Attorney General have certified that a significant purpose of the acquisition is to obtain foreign intelligence information;

(4) each authorization for the acquisition of targeted United States person communications is limited to 90 days;

(5) there are reasonable minimization procedures in place, which meet the definition of "minimization procedures" under 50 U.S.C.A. § 1801(h); and

(6) there are written procedures in place to ensure that surveillance of the facilities to be targeted likely will obtain foreign intelligence information,

this Court is satisfied that the government currently has in place sufficient procedures to ensure that the Fourth Amendment rights of targeted United States persons are adequately protected and that the acquisition of the foreign intelligence to be obtained through the directives issued to Yahoo, as to these individuals, is reasonable under the Fourth Amendment. ~~(S)~~

e. The Reasonableness of Incidentally Acquiring Communications of United States Persons (U)

The previous section of this Opinion concerned the Fourth Amendment rights of those United States persons whose communications are targeted. However, the universe of communications that will be acquired through the directives issued to Yahoo will include the communications of persons who communicate with the targeted accounts.[88] Yahoo argues, Yahoo's Mem. in Opp'n at 9, and the government concedes, "[t]he directives therefore, implicate, to varying degrees, the Fourth Amendment rights of ... persons, whether abroad or inside the United States, who are communicating with foreign intelligence targets outside the United States." Gov't.'s Supp. Brief on the Fourth Amend. at 2. This Court agrees that some subset of non-target communicants located in the United States and non-target communicants who are United States persons, whether located in the United States or abroad, enjoy Fourth Amendment protection. United States v. Verdugo-Urquidez, 494 U.S. 259. ~~(S)~~

As the District Court in Bin Laden noted, "... incidental interception of a person's conversations during an otherwise lawful surveillance is not violative of the Fourth Amendment." 126 F. Supp. 2d at 280 (citations omitted). Likewise, the Second Circuit has held,

[88] It is this Court's understanding that the directives issued to Yahoo will result in the acquisition of non-target communications only if the non-targeted account is in direct communication with a targeted account or if a communication of the non-targeted account is forwarded to a targeted account. See Declaration of [redacted] January 16, 2008; Declaration of [redacted] January 23, 2008. ~~(S)~~

"[i]f probable cause has been shown as to one such participant, the statements of the other participants may be intercepted if pertinent to the investigation." United States v. Tortorello, 480 F.2d 764, 775 (2d Cir. 1973). As discussed earlier in this opinion, supra Part II, this Court has found that the acquisition of communications obtained through the directives issued to Yahoo adheres to the requirements of the PAA. And, as discussed immediately above, this Court has found that the acquisition of the communications of targeted United States persons obtained through the directives issued to Yahoo is reasonable and therefore complies with the Fourth Amendment. ~~(S)~~

This Court also notes that, in addition to the underlying surveillance being lawful, the government has in place minimization procedures designed to protect the privacy interests of United States persons. As required by the PAA, the government must have procedures in place that comport with the definition of minimization procedures under section 1801(h) of FISA. That definition specifies that such procedures must be

> (1) specific procedures ... reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
>
> (2) procedures that require that nonpublicly available information, which is not foreign intelligence information ... shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance[.]

50 U.S.C.A. § 1801(h)(1) & (2) (emphasis added). This Court agrees with the government that these minimization procedures adequately protect the privacy interests of persons whose

communications might be incidentally acquired. Mem. in Support of Gov't Motion at 19; see also Feb. 2008 Classified Appendix at [redacted] (u)

Based on the above considerations, this Court finds that any incidental acquisition of the communications of non-targeted persons located in the United States and of non-targeted United States persons, wherever they may be located, is also reasonable under the Fourth Amendment. (u)

IV. Conclusion (u)

There are times when there is an inevitable tension between the interests protected by the Fourth Amendment on the one hand and the federal government's obligation to protect the security of the nation on the other hand. This reality has been particularly acute in an era of ever increasing communications and intelligence technology, when at the same time the threat of global terrorism has intensified, ultimately reaching the American mainland with devastating consequences on September 11, 2001. That is the landscape which confronted the United States Congress when the legislation that is the subject of this Opinion was enacted. Congress obviously sought to strike the proper balance between the sometime conflicting interests of individual privacy and national security when it the adopted the PAA. But as illustrated by the painstaking and complex constitutional and statutory analysis this Court had to conduct to resolve the dispute in this case, the balance is not easily achieved. Despite the concerns the Court has expressed regarding several aspects of the legislation, for the reasons set forth above, this Court finds that the directives issued by the government to Yahoo satisfy the requirements of the PAA, do not offend the Fourth Amendment, and are otherwise lawful. Accordingly, Yahoo is instructed to comply with the directives and an Order directing Yahoo to do so is being issued contemporaneously with this Opinion. (S)

ENTERED this 25th day of April, 2008 in Docket Number 105B(g): 07-01. (S)

REGGIE B. WALTON
Judge, Foreign Intelligence Surveillance Court

Classified by: Mark A. Bradley
National Security Division
U.S. Department of Justice

Declassify on: April 29, 2033

Filed [redacted]
CSO: [redacted]
DATE: 4-25-08

~~SECRET~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

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

Docket Number 105B(g): 07-01 (S)

ORDER COMPELLING COMPLIANCE WITH DIRECTIVES (S)

This case comes before the Court on the government's motion pursuant to 50 U.S.C.A. § 1805b(g) (West Oct. 2007) to compel compliance with [redacted] directives it issued to Yahoo!, Inc. (Yahoo) pursuant to the Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (PAA).[1] These directives issued to Yahoo were signed by the Acting Attorney General on November 6, 2007, and the Director of National Intelligence on November 7, 2007, pursuant to [redacted]

[1] The PAA amended the Foreign Intelligence Surveillance Act (FISA) (which, in its present form, can be found at 50 U.S.C.A. §§ 1801-1871 (West 2003, Supp. 2007 & Oct. 2007)). As originally enacted, the PAA had a "sunset" provision, under which its substantive terms would "cease to have effect 180 days after the date of the enactment" of the PAA, subject to certain exceptions applicable to this case. PAA § 6(c). On January 31, 2008, Congress extended this period to "195 days after the date of the enactment of [the original PAA]." See Pub. L. 110-182, § 1, 122 Stat. 605. Congress took no further action, and this 195-day period expired on February 16, 2008. (U)

~~SECRET~~

3. The determination of lawfulness stated in paragraph 1. above is also predicated on certain assumptions that the Court has made in the Memorandum Opinion regarding the process whereby acquisitions targeting United States persons are approved by the Attorney General under section 2.5 of Executive Order No. 12,333, 3 C.F.R. 200 (1982), reprinted as amended in 50 U.S.C. § 401 (2000 & Supp. V 2005).[3] Specifically, the Court has assumed that:

(a) the government will follow the section 2.5 procedures whenever it is reasonable to believe that the target is a United States person; and

(b) after the initial authorization under section 2.5 to target a U.S. person, the Attorney General must re-authorize the acquisition every 90 days in order for acquisition to continue, and if the Attorney General does not issue a new authorization after 90 days, acquisition for a targeted account used by a United States person will cease.[4] ~~(S)~~

Accordingly, it is further ORDERED that, on or before May 9, 2008, the government shall apprise the Court, by written submission in the above-captioned docket, in the event that either of the above-stated assumptions is not correct. ~~(S)~~

It is further ORDERED that, in the event that the government changes how it implements the section 2.5 process regarding accounts to be identified for acquisition under the above-referenced directives issued to Yahoo in a manner that would render either of the above-stated

---

[3]This section 2.5 process does not apply to acquisitions targeting non-United States persons. (U)

[4]The Court believes that these assumptions are correct; however, the government's submissions are not entirely clear on these points. Rather than delaying the issuance of this Order pending clarification of a process applicable only to the subset of acquisitions targeting United States persons, the Court has decided to issue this Order based on the above-stated assumptions, subject to a requirement that the government promptly inform the Court if either assumption is not correct. ~~(S)~~

assumptions incorrect, the government shall forthwith apprise the Court of such change by written submission in the above-captioned docket. ~~(S)~~

It is further ORDERED that because the Memorandum Opinion discusses classified information submitted to the Court for ex parte and in camera review pursuant to 50 U.S.C. § 1805b(k), it shall be reviewed for proper classification prior to being served on counsel for Yahoo. Such review shall be conducted in accordance with paragraph 2 of this Court's Order Establishing Procedures for Handling Classified Information, entered in this matter on December 28, 2007. ~~(S)~~

It is further ORDERED that, as expeditiously as possible, and no later than May 14, 2008, a copy of the Memorandum Opinion, appropriately marked for classification and redacted as necessary, shall be served on counsel for Yahoo. A copy of the Memorandum Opinion as served on counsel for Yahoo shall also be filed with the Court. (S)

It is further ORDERED that this Order and the Memorandum Opinion are sealed and shall not be disclosed by either party without authorization by this Court. (U)

ENTERED this 25th day of April, 2008 in Docket Number 105B(g): 07-01. (S)

REGGIE B. WALTON
Judge, Foreign Intelligence Surveillance Court

Classified by: Mark A. Bradley
National Security Division
U.S. Department of Justice

Declassify on: April 29, 2033