

~~TOP SECRET//COMINT//ORCON,NOFORN~~

No. 08-01 (S)
IN THE UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW (U)

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

ON PETITION FOR REVIEW OF A DECISION OF THE
UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT (U)

EX PARTE BRIEF FOR RESPONDENT (S)

Michael B. Mukasey
Attorney General

Mark Filip
Deputy Attorney General

J. Patrick Rowan
Acting Assistant Attorney General

John A. Eisenberg
Office of the Deputy Attorney General


Office of Legal Counsel


Civil Division

Matthew G. Olsen
John C. Demers


National Security Division

United States Department of Justice

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Classified by:

Matthew G. Olsen, Deputy Assistant
Attorney General, NSD, DOJ

Reason:

1.4 (c)

Declassify on:

5 June 2033

~~TOP SECRET//COMINT//ORCON,NOFORN~~

TABLE OF CONTENTS (U)

INTRODUCTION (U)	1
STATEMENT OF JURISDICTION (U)	3
STATEMENT OF THE ISSUES (U)	4
STATEMENT OF THE CASE (U)	5
STATEMENT OF THE FACTS (U)	5
A. Foreign Intelligence Surveillance and FISA (U)	5
B. The Protect America Act (U)	9
C. Implementation of the Protect America Act (U)	12
D. Proceedings Before the FISC (S)	14
STANDARD OF REVIEW (U)	17
SUMMARY OF ARGUMENT (U)	17
ARGUMENT (U)	21
I. THE ACQUISITION OF FOREIGN INTELLIGENCE INFORMATION UNDER THE CHALLENGED DIRECTIVES IS LAWFUL UNDER THE FOURTH AMENDMENT (S)	21
A. The Fourth Amendment's Warrant Requirement Does Not Apply to the Collection of Foreign Intelligence Information Under the Challenged Directives. (S)	23
1. A Judicial Warrant Is Not Required For the Collection of Foreign Intelligence Information. (U)	23
2. The Acquisition of Foreign Intelligence Information Under the Directives Falls Squarely Within the Foreign Intelligence Exception to the Warrant Requirement. (S)	28

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

B. The Government's Collection of Foreign Intelligence Information Pursuant to the Directives Is Reasonable Under The Fourth Amendment. (S)	34
1. Acquisitions Under The Directives Advance the Government's Compelling Interest in Obtaining Foreign Intelligence Information To Protect National Security	34
2. The Privacy Interests of U.S. Persons Are Protected by Stringent Safeguards and Procedures. (S)	35
a. The Attorney General must make a probable cause determination under E.O. 12333. (S)	36
b. Senior officials certify that the Government's procedures satisfy statutory requirements. (S)	38
c. Targeting procedures ensure that the Government targets only persons reasonably believed to be outside the United States. (S)	39
d. Minimization procedures protect the privacy of U.S. persons whose communications are acquired. (S)	40
e. A significant purpose of the acquisition must be to obtain foreign intelligence information. (S)	41
3. The Absence of Other Factors Does Not Render the Acquisitions Unreasonable. (S)	42
a. Prior court approval for each target is not required. (S)	43
b. The methods used to identify the facilities to be targeted are reasonable. (S)	46
4. The Incidental Collection of Communications of U.S. Persons Does Not Violate the Fourth Amendment. (S)	49
II. YAHOO MAY NOT CHALLENGE THE DIRECTIVES ON THE BASIS THAT THEY VIOLATE THE FOURTH AMENDMENT RIGHTS OF THIRD PARTIES (S)	53
CONCLUSION (U)	56

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

CERTIFICATE OF SERVICE (U)

CERTIFICATE OF COMPLIANCE (U)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

TABLE OF AUTHORITIES (U)

CASES

<u>Alderman v. United States</u> , 394 U.S. 165 (1969)	53
<u>ACLU v. National Security Agency</u> , 493 F.3d 644 (6th Cir. 2007), <u>cert. denied</u> , 128 S. Ct. 1334 (Feb. 19, 2008)	54
<u>Bennett v. Spear</u> , 520 U.S. 154 (1997)	55
<u>Berger v. New York</u> , 388 U.S. 41 (1967)	47
<u>Board of Educ. v. Earls</u> , 536 U.S. 822 (2002)	24
<u>California Bankers Ass'n v. Schultz</u> , 416 U.S. 21 (1974)	53, 54, 55
<u>Cannon v. University of Chicago</u> , 441 U.S. 677 (1979)	31
<u>Cassidy v. Chertoff</u> , 471 F.3d 67 (2d Cir. 2006)	25
<u>City of Indianapolis v. Edmond</u> , 531 U.S. 32 (2001)	24, 28, 29, 30
<u>Coolidge v. New Hampshire</u> , 403 U.S. 443 (1971)	44
<u>Dames & Moore v. Regan</u> , 453 U.S. 654 (1981)	38
<u>Daimler Chrysler v. Cuno</u> , 547 U.S. 332 (2006)	54
<u>Ellwest Stereo Theatres, Inc. v. Wenner</u> , 681 F.2d 1243 (9th Cir. 1982)	54
<u>Graham v. Connor</u> , 490 U.S. 386, 396 (1989)	42
<u>Griffin v. Wisconsin</u> , 483 U.S. 868 (1987)	23, 24, 44
<u>Griswold v. Connecticut</u> , 381 U.S. 479 (1965)	56
<u>Haig v. Agee</u> , 453 U.S. 280 (1981)	34
<u>Haitian Refugee Ctr. v. Gracey</u> , 809 F.2d 794 (D.C. Cir. 1987)	56
<u>Hollingsworth v. Hill</u> , 110 F.3d 733 (10th Cir. 1997)	54
<u>Illinois v. Lafayette</u> , 462 U.S. 640 (1983)	51

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

<u>In re Sealed Case</u> , 310 F.3d 717 (FISA Ct. Rev. 2002)	<i>passim</i>
<u>Kowalski v. Tesmer</u> , 543 U.S. 125 (2004)	54, 56
<u>Lackawanna County Dist. Attorney v. Coss</u> , 532 U.S. 394 (2001)	4
<u>MacWade v. Kelly</u> , 460 F.3d 260 (2d Cir. 2006)	25
<u>Minnesota v. Carter</u> , 525 U.S. 83 (1998)	53
<u>National Treasury Employees Union v. Von Raab</u> , 489 U.S. 656 (1989)	24, 32
<u>New Jersey v. T.L.O.</u> , 469 U.S. 325 (1985)	24
<u>Pierce v. Society of Sisters</u> , 268 U.S. 510 (1925)	56
<u>Pasiewicz v. Lake County Forest Preserve Dist.</u> , 270 F.3d 520 (7th Cir. 2001) ...	49
<u>Rakas v. Illinois</u> , 439 U.S. 128 (1978)	53, 55
<u>Skinner v. Railway Labor Executives' Ass'n</u> , 489 U.S. 602 (1989)	24, 34
<u>South Dakota v. Opperman</u> , 428 U.S. 364 (1976)	55
<u>Swan v. Clinton</u> , 100 F.3d 973 (D.C. Cir. 1996)	4
<u>Thunder Basin Coal Co. v. Reich</u> , 510 U.S. 200 (1994)	4
<u>United States v. Bin Laden</u> , 126 F. Supp. 2d 264 (S.D.N.Y. 2000)	
.....	16, 25, 30, 37, 45, 50
<u>United States v. Brown</u> , 484 F.2d 418 (5th Cir. 1973)	26, 50
<u>United States v. Buck</u> , 548 F.2d 871 (9th Cir. 1977)	26
<u>United States v. Butenko</u> , 494 F.2d 593 (3d Cir. 1974)	26, 50
<u>United States v. Carter</u> , 413 F.3d 712 (8th Cir. 2005)	47
<u>United States v. Figueroa</u> , 757 F.2d 466 (2d Cir. 1985)	50
<u>United States v. Hutchinson</u> , 408 F.3d 796 (D.C. Cir. 2005)	17
<u>United States v. Kahn</u> , 415 U.S. 143 (1974)	50

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

<u>United States v. Knights</u> , 534 U.S. 112 (2001)	34
<u>United States v. Martinez-Fuerte</u> , 428 U.S. 543 (1976)	24, 47
<u>United States v. Posey</u> , 864 F.2d 1487 (9th Cir. 1989)	33
<u>United States Postal Serv. v. Gregory</u> , 534 U.S. 1 (2001)	49
<u>United States v. Redmon</u> , 138 F.3d 1109 (7th Cir. 1998)	42
<u>United States v. Sargent</u> , 319 F.3d 4 (1st Cir. 2003)	17
<u>United States v. Tortorello</u> , 480 F.2d 764 (2d Cir. 1973)	50
<u>United States v. Truong Dinh Hung</u> , 629 F.2d 908 (4th Cir. 1980)	25, 26, 28
<u>United States v. United States Dist. Court</u> , 444 F.2d 651 (6th Cir. 1971)	5
<u>United States v. United States Dist. Court (Keith)</u> , 407 U.S. 297 (1972)	27, 28, 44
<u>United States v. Verdugo-Urquidez</u> , 494 U.S. 259 (1990)	21, 22
<u>Vernonia Sch. Dist. 47J v. Acton</u> , 515 U.S. 646 (1995)	23, 24, 32
<u>Warth v. Seldin</u> , 422 U.S. 490 (1975)	54
<u>Youngstown Sheet & Tube Co. v. Sawyer</u> , 343 U.S. 579 (1952)	52
<u>Zweibon v. Mitchell</u> , 516 F.2d 594 (D.C. Cir. 1975)	28

CONSTITUTION AND STATUTES

U.S. CONST. amend. IV	<i>passim</i>
28 U.S.C. § 1653	3
50 U.S.C. § 1801(b)(1)(A)	6
50 U.S.C. § 1801(b)(2)(C).....	6
50 U.S.C. § 1801(f)(1).....	7

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

50 U.S.C. § 1801(f)(2).....	7, 8, 9
50 U.S.C. § 1801(f)(3).....	7, 8, 9
50 U.S.C. § 1801(f)(4).....	7, 8, 9
50 U.S.C. § 1801(h).....	11, 40
50 U.S.C. § 1801(h)(1).....	4, 6
50 U.S.C. § 1801(i).....	6
50 U.S.C. § 1803(b).....	4
50 U.S.C. § 1804	7, 37
50 U.S.C. § 1804(a).....	4, 6
50 U.S.C. § 1805	6, 7, 27, 37
50 U.S.C. § 1805A	1, 10
50 U.S.C. § 1805B.....	3, 4
50 U.S.C. § 1805B(a)	10, 39
50 U.S.C. § 1805B(a)(1)	11, 38, 39
50 U.S.C. § 1805B(a)(4)	29, 41
50 U.S.C. § 1805B(a)(5)	40
50 U.S.C. § 1805B(d)	42
50 U.S.C. § 1805B(e)	5, 11, 15, 54
50 U.S.C. § 1805B(g)	3, 14, 21, 33, 54
50 U.S.C. § 1805B(h)	3
50 U.S.C. § 1805B(h)(1)	4
50 U.S.C. § 1805B(i).....	3, 4
50 U.S.C. § 1805B(k)	12

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

50 U.S.C. § 1805C(b)	11
50 U.S.C. § 1823	37
50 U.S.C. § 1824	37
Protect America Act of 2007, Pub. L. 110-55, 121 Stat. 552 (Aug. 5, 2007).....	<i>passim</i>
MISCELLANEOUS	
Exec. Order No. 12333, § 2.5, 46 Fed. Reg. 59,941 (Dec. 4, 1981)	
.....	13, 29, 32, 36, 37
153 Cong. Rec. S10,857 (Aug. 3, 2007)	26
H.R. Rep. No. 95-1283, 95 th Cong., 2d Sess. (1978)	6, 7, 8
S. Rep. No. 110-209, 110 th Cong., 1 st Sess. (2007).....	10
<u>Department of Defense Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons</u> , 5240.1-R, p. 5, pt. 2.C (Dec. 1982)	13, 22, 36, 37, 51

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

INTRODUCTION (U)

This case presents a challenge to the Government's authority to conduct critical foreign intelligence surveillance targeting persons outside the United States as explicitly authorized by Congress in the Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552, codified at 50 U.S.C. §§ 1805A-1805C ("Protect America Act"). The Government has conducted warrantless foreign intelligence surveillance for decades, and such surveillance has been upheld under the Fourth Amendment by every appellate court to decide the question. Consistent with this long-standing and uniform precedent, the Foreign Intelligence Surveillance Court ("FISC") found lawful [REDACTED] directives the Government issued to Yahoo!, Inc. ("Yahoo") pursuant to the Protect America Act. That statute was specifically intended to address the significant challenges the Government faced in collecting foreign intelligence as a result of sweeping changes in communications technology following the enactment of the Foreign Intelligence Surveillance Act ("FISA") in 1978. (S)

As the attacks of September 11, 2001, have underscored, timely and accurate foreign intelligence information on the intentions and capabilities of our adversaries is a crucial tool in the fight against international terrorism. The Government requires the assistance of communications service providers to acquire this information, and [REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED]

[REDACTED] (S)

Yahoo's constitutional challenge to the directives issued by the Government is without merit. Those directives—issued pursuant to the Executive Branch's inherent authority to conduct foreign intelligence surveillance and the express authorization of Congress—fully satisfy Fourth Amendment requirements. Because the foreign intelligence surveillance at issue falls within an exception to the Warrant Clause of the Fourth Amendment, the surveillance is required only to satisfy the constitutional requirement of reasonableness. Here, the Government's implementation of the Protect America Act is consistent with decades of past practice and adequately protects the privacy of U.S. persons. In particular, the Attorney General must approve any surveillance targeting a U.S. person abroad, and only after finding that the person is a foreign power or agent of a foreign power. The Government employs extensive procedures to ensure that the surveillance is appropriately targeted and to minimize the acquisition, retention, and dissemination of information in order to protect the privacy of U.S. persons. (S)

These and other safeguards ensure that the acquisition of foreign intelligence information under the Protect America Act meets Fourth Amendment standards. There is, accordingly, no basis for this Court to overturn the judgment of Congress

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

and the Executive with respect to the foreign intelligence surveillance activities at issue. This Court should affirm the judgment of the FISC. ~~(S)~~

STATEMENT OF JURISDICTION (U)

The FISC had jurisdiction over the Government's motion to compel Yahoo's compliance with the directives issued to it pursuant to 50 U.S.C. § 1805B(g). On April 25, 2008, the FISC granted the Government's motion and ordered Yahoo to comply forthwith. Yahoo filed a timely petition for review on May 5, 2008. ~~(S)~~

Although the question is not free from doubt, this Court appears to have jurisdiction over Yahoo's petition for review under 50 U.S.C. § 1805B. If the FISC had denied the Government's motion to compel compliance with the challenged directives, the Government's position is that this Court would have jurisdiction to review the order, and the same principle would appear to permit review of an order compelling compliance. The FISC's order rejecting Yahoo's challenge to the lawfulness of the directives may be treated as the functional equivalent to a ruling on a petition to modify or set aside a directive under § 1805B(h), which § 1805B(i) expressly gives this Court jurisdiction to review. Cf. In re Sealed Case, 310 F.3d 717, 721 (FISA Ct. Rev. 2002) (refusing to "elevate form over substance" in construing jurisdictional provision of FISA). Pursuant to 28 U.S.C. § 1653, this Court may amend "[d]efective allegations of jurisdiction" in Yahoo's opposition to the Government's motion to clarify that it constituted a

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

challenge to the directives pursuant to § 1805B(h)(1), and similarly to amend Yahoo's petition for review to invoke this Court's jurisdiction under 50 U.S.C. § 1805B(i). See, e.g., Swan v. Clinton, 100 F.3d 973, 980 & n.3 (D.C. Cir. 1996).¹

~~(S)~~

STATEMENT OF THE ISSUES (U)

1. Whether the Government's acquisition of foreign intelligence information pursuant to the challenged directives complies with the Fourth Amendment. ~~(S)~~

2. Whether Yahoo may vicariously raise the rights of third parties in challenging the directives under the Fourth Amendment. ~~(S)~~

¹ Contrary to Yahoo's suggestion, this Court does not have jurisdiction to review the FISC's order pursuant to 50 U.S.C. § 1803(b). See Yahoo Br. 1. That section confers jurisdiction "to review the denial of any application made under this Act," i.e., the denial of an application by the Government for judicial authorization to conduct surveillance under provisions such as § 1804(a). No "application"—a term not used in § 1805B—has been made in this case, much less denied. Due process principles also have no bearing on the jurisdictional question. Apart from the fact that there is no constitutional right to appeal even a criminal conviction, see, e.g., Lackawanna County Dist. Atty. v. Coss, 532 U.S. 394, 402-403 (2001), and that Yahoo has no constitutional right to challenge an alleged violation of third parties' Fourth Amendment rights, see infra pp. 53-56, there is no constitutional impediment to requiring a litigant to use a specific and exclusive review process. See, e.g., Thunder Basin Coal Co. v. Reich, 510 U.S. 200, 216-218 (1994). ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

STATEMENT OF THE CASE (U)

Pursuant to 50 U.S.C. § 1805B(e), the Director of National Intelligence (“DNI”) and the Attorney General issued [REDACTED] directives requiring Yahoo to assist the Government in acquiring foreign intelligence information concerning certain persons reasonably believed to be outside the United States. Joint Appendix (“J.A.”) 21-26. The Government moved in the FISC for an order compelling Yahoo’s compliance. J.A. 12-26. The FISC granted the Government’s motion and ordered Yahoo to comply with the directives. J.A. 217-20. The case is before this Court on Yahoo’s petition for review of the FISC’s order. (S)

STATEMENT OF THE FACTS (U)

A. Foreign Intelligence Surveillance and FISA (U)

Since the earliest years of this country, the Government has relied on foreign intelligence collection to protect the nation. For the vast majority of that time and through the present day, much of this intelligence gathering has been conducted under the President’s constitutional authority over national security and foreign affairs, with the methods of surveillance adapted over time in light of developing technologies. Presidents have authorized wiretaps for foreign intelligence purposes since at least 1940. See, e.g., United States v. United States Dist. Court, 444 F.2d 651, 669-71 (6th Cir. 1971) (reproducing as an appendix memoranda from Presidents Roosevelt, Truman, and Johnson). (U)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

In 1978, Congress enacted FISA to establish a “statutory procedure authorizing the use of electronic surveillance in the United States for foreign intelligence purposes.” H.R. Rep. No. 95-1283, 95th Cong., 2d Sess. (1978), at 22. Where FISA applies, it generally requires the Attorney General to apply to the FISC for an order approving the use of “electronic surveillance” to “obtain foreign intelligence information,” 50 U.S.C. § 1804(a), which is defined to include information necessary to protect against espionage, international terrorism, and other acts committed by foreign powers or their agents, as well as other information pertaining to the national defense and foreign affairs of the United States. Id. § 1801(e). As a condition of approval, the FISC must find that the applicant establishes probable cause to believe that the target of electronic surveillance is a foreign power or an agent of a foreign power, see id. §§ 1801(b)(1)(A), (b)(2)(C), (i), and that the target is using or is about to use the facility at which surveillance will be directed. Id. § 1805. The judge must also find that “minimization procedures” proposed by the Government are, inter alia, “reasonably designed . . . 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.” Id. §§ 1801(h)(1), 1805(a)(4). (U)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Congress drafted FISA to exclude from the judicial approval requirement the majority of foreign intelligence surveillance directed overseas at the time. Under FISA, only “electronic surveillance” is subject to the requirement of prior judicial approval, see 50 U.S.C. §§ 1804, 1805, and the statute’s definition of “electronic surveillance” excluded much surveillance directed overseas even where conducted in the United States, see id. § 1801(f)(1). In relevant part, the first definition of “electronic surveillance” is the acquisition of a “wire or radio communication” to or from “a particular, known United States person who is in the United States . . .” Id. § 1801(f)(1) (emphasis added). The second definition relates to the acquisition of a “wire communication,” § 1801(f)(2)—which is defined as a communication carried on a wire by “common carriers.” As of 1978, this excluded most international communications, which at that time were carried primarily by satellite (i.e., radio). See id. This definition requires that only one end of the communications be in the United States (and that the acquisition occur within the United States). In contrast, the third definition of “electronic surveillance” applies to the acquisition of a “radio communication” only when “both the sender and all intended recipients are located within the United States.” Id. § 1801(f)(3). The final definition covers the use “of an electronic, mechanical, or other surveillance device in the United States,” but expressly excludes the acquisition of information from any “wire or radio communication.” Id. § 1801(f)(4); see also H.R. Rep. No.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

95-1283, at 52 (explaining that § 1801(f)(4) was “not meant to include . . . the acquisition of those international radio transmissions which are not acquired by targeting a particular U.S. person in the United States”). Accordingly, at the time FISA was enacted, most foreign-to-foreign and international communications fell outside the definition of “electronic surveillance.” (U)

Transformative changes in communications technology after 1978 upended FISA’s treatment of intelligence activities directed at persons overseas. By 2007, most international communications traveled by fiber optic cable (“wire”) rather than by satellite (“radio”). The effect of this change was to bring within the scope of FISA many communications that, as of 1978, would have fallen outside it. Compare § 1801(f)(2) (defining wire communication as “electronic surveillance” if, inter alia, one party is in the United States) with § 1801(f)(3) (defining radio communication as “electronic surveillance” only if sender and all intended recipients are in the United States). (U)

In addition, new communications methods, such as e-mail, did not exist (or were not commonly used) in 1978. FISA’s definitions have come to include many of these communications without regard to the location of the parties. For example, [REDACTED] the Government’s e-mail collection under FISA takes place at Internet service providers (ISPs) in the United States. Collection of e-mail at these ISPs falls under the definition of electronic surveillance in § 1801(f)(4) (because these

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

ISPs are generally not operating as common carriers) even if the e-mails collected are sent to and received by foreigners located outside the United States. Unlike the section applicable to wire communications (§ 1801(f)(2)), which excludes communications where all parties are known to be located outside the United States (i.e., foreign-to-foreign communications), and the section applicable to radio communications (§ 1801(f)(3)) which excludes communications where any party is outside the United States), the section applicable to collections at ISPs (§ 1801(f)(4)) does not include such a carve out. See 50 U.S.C. § 1801(f). Thus, technological changes have served to expand greatly FISA's coverage of the type of traditional foreign intelligence collection that had long been conducted, with Congress's knowledge, outside FISA, and did so without any consideration by Congress. ~~(TS//SI//NF)~~

B. The Protect America Act (U)

The expansion of FISA's scope and the nature of the threat facing the United States created a gap between the foreign telephone numbers and e-mail addresses that the Government needed to surveil and the Government's ability to meet the statutory requirements to secure court orders under FISA. Responding to this concern, Congress amended FISA in 2007 through enactment of the Protect America Act. The Act sought to facilitate the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

by eliminating “the requirement of a court order to collect foreign intelligence information about targets located overseas.” S. Rep. No. 110-209, 110th Cong., 1st Sess., at 2, 5-6 (2007). This modification was intended to bring FISA “up to date with the changes in communications technology” and to address the “degraded capabilities in the face of a heightened terrorist threat environment,” while at the same time preserving “the privacy interests of persons in the United States.” Id. (U)

With respect to targets outside the United States, the Protect America Act made FISA’s definition of “electronic surveillance” focus exclusively on the location of the target rather than also on the location of the surveillance or the type of communication at issue. The Protect America Act thus excluded from FISA’s electronic surveillance definition “surveillance directed at a person reasonably believed to be located outside of the United States,” 50 U.S.C. § 1805A, thereby returning the scope of FISA’s electronic surveillance definition closer to its scope in 1978. The Protect America Act empowered the DNI and the Attorney General jointly to “authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside of the United States” for up to one year, id. § 1805B(a), and to issue directives to communications service providers requiring them to “immediately provide the Government with all information,

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

facilities, and assistance necessary to accomplish the acquisition,” id. § 1805B(e).²

(U)

To ensure that acquisitions intentionally target only persons outside the United States, and to protect the privacy of U.S. persons, the Protect America Act required the DNI and Attorney General to certify, inter alia, that there are reasonable procedures in place for determining that the acquisition concerns persons reasonably believed to be located outside the United States (“targeting procedures”), see 50 U.S.C. § 1805B(a)(1); there are minimization procedures in place that satisfy FISA’s requirements for such procedures, see id. § 1801(h); and a significant purpose of the acquisition is to acquire foreign intelligence information. Id. § 1805B(a)(1), (4), and (5). The Act also authorized the FISC to review the DNI and the Attorney General determination regarding the reasonableness of the targeting procedures. Id. § 1805C(b). Pursuant to that provision, the FISC subsequently reviewed the targeting procedures approved by the DNI and the

² As originally enacted, portions of the Protect America Act were scheduled to sunset 180 days from the date of enactment. Congress later passed a 15-day extension of the Protect America Act, so portions of the Protect America Act did not actually sunset until February 16, 2008. As recognized by the FISC, the expiration of those certain provisions did not affect the validity of the directives or the FISC’s jurisdiction to compel compliance. J.A. 122-29. See 121 Stat. 552, § 6(d) (“Authorizations for the acquisition of foreign intelligence information pursuant the amendments made by this Act, and directives pursuant to such authorizations, shall remain in effect until their expiration. Such acquisitions shall be governed by the applicable provisions of such amendments.”). ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Attorney General and upheld them. See In re DNI/AG Certification [REDACTED]

[REDACTED] (FISA Ct. Jan. 15, 2008), Government's Ex Parte Appendix ("E.A.") 557-651; see also [REDACTED] (NSA targeting procedures on file with the FISC).³ (S)

C. Implementation of the Protect America Act (U)

In August and September 2007, the DNI and the Attorney General executed [REDACTED] certifications for the acquisition of foreign intelligence information concerning: [REDACTED]

[REDACTED] Each authorization contains the certifications required by the Protect America Act and is in effect for a period of one year from the date of authorization.

[REDACTED] (S)

³ Pursuant to 50 U.S.C. § 1805B(k), the Government requests that the Court review ex parte and in camera the certifications, declarations, and other information contained in the Ex Parte Appendix. The Government previously submitted these documents for the FISC's ex parte and in camera review. [REDACTED]

[REDACTED] Because Yahoo's counsel is not cleared to review certain information in this brief and the Ex Parte Appendix, the Government, as it did in the FISC, will serve counsel with copies of any documents redacted in accordance with requirements for the protection of classified information. (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~


~~TOP SECRET//COMINT//ORCON,NOFORN~~


The DNI and the Attorney General further certified that, before an acquisition may target a U.S. person located outside the United States, the Government “must first obtain Attorney General authorization, using the procedures under Executive Order 12333, section 2.5.” E.A. 5, 39, 87, 141-42, 188, 226. Section 2.5 of Executive Order 12333 authorizes the Attorney General to approve “the use for intelligence purposes . . . against a U.S. person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes.” Exec. Order No. 12333, § 2.5, 46 Fed. Reg. 59,941 (Dec. 4, 1981) (as amended); J.A. 263. The Attorney General may authorize such surveillance only when he “determine[s] in each case that there is probable cause to believe that the [surveillance] technique is directed against a foreign power or an agent of a foreign power.” *Id.* Under longstanding Department of Defense procedures implementing section 2.5 and applicable here, such authorizations last only 90 days. Department of Defense Procedures Governing the Protect America Activities of DoD Intelligence Components That Affect United States Persons, DoD 5240.1-R, Proc. 5, Pt. 2.C (“DoD Procedures”); J.A. 61-62. (S)

Pursuant to authorizations under the Protect America Act, the DNI and the Attorney General issued directives to communications service providers requiring their assistance. After extensive discussions with Yahoo, the Government served [REDACTED] directives on the company in November 2007. J.A. 21-26. Yahoo refused to

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

comply with the directives, and the Government initiated proceedings in the FISC to compel compliance. As the Government subsequently elaborated in a declaration filed by the DNI, Yahoo's compliance with the directives 

~~(TS//SI//NF)~~

D. Proceedings Before the FISC ~~(S)~~

Yahoo opposed the Government's motion to compel compliance under 50 U.S.C. § 1805B(g), primarily on the ground that the directives violated the Fourth

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Amendment rights of its customers. J.A. 27-58. On April 25, 2008, following extensive briefing by the parties, the FISC held that the directives issued to Yahoo “do not offend the Fourth Amendment, and were issued in accordance with [50 U.S.C. § 1805B(e)] and [are] otherwise lawful.” J.A. 215. The FISC ordered Yahoo to “forthwith comply with the directives, and [to] continue to comply with each directive until the expiration date specified therein.” J.A. 218. (S)

The FISC rejected Yahoo’s arguments, including its claim that the directives violate the Fourth Amendment because they authorize the acquisition of U.S. person communications without a warrant. The FISC reasoned that this Court necessarily recognized the existence of a foreign intelligence exception to the Fourth Amendment’s Warrant Clause in upholding electronic surveillance under FISA in In re Sealed Case. J.A. 174-77. Relying on that decision, the FISC held that the foreign intelligence exception applies if a “significant purpose” of the acquisition is to acquire foreign intelligence information and “a sufficiently authoritative official [finds] probable cause to believe that the target of the search or electronic surveillance is a foreign power or its agent.” J.A. 177-86; E.A. 337-46. Because the certifications made by the Attorney General and the DNI meet these standards, the FISC held that the directives fell within the foreign intelligence exception to the Fourth Amendment’s warrant requirement. J.A. 186; E.A. 346. (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

CR 0099

The FISC also held that the directives satisfied the Fourth Amendment's requirement of reasonableness. The FISC analyzed In re Sealed Case and United States v. Bin Laden, 126 F. Supp. 2d 264 (S.D.N.Y. 2000). Both cases concerned the acquisition of communications of U.S. persons for foreign intelligence purposes, but differed in one important respect. Bin Laden, like this case, concerned an acquisition targeted at a U.S. person located outside the United States, whereas In re Sealed Case concerned the electronic surveillance of a U.S. person located within the United States. J.A. 190-98; E.A. 350-58. The FISC ultimately held, based on its analysis of those decisions and the totality of the circumstances in this case, that the Government had sufficient procedures in place "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." J.A. 212-13. (S)

The FISC subsequently denied a stay pending appeal and, because Yahoo had still not provided the required assistance, ordered Yahoo's compliance upon threat of contempt. J.A. 244-45. This Court deferred ruling on Yahoo's motion for a stay in this Court, pending the completion of expedited briefing on the merits and any oral argument. (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

STANDARD OF REVIEW (U)

The FISC's determination that acquisitions authorized under the challenged directives satisfy the Fourth Amendment is reviewed de novo. See, e.g., United States v. Hutchinson, 408 F.3d 796, 798 (D.C. Cir. 2005); United States v. Sargent, 319 F.3d 4, 8 (1st Cir. 2003). ~~(S)~~

SUMMARY OF ARGUMENT (U)

I. Congress and the Executive Branch have authorized the acquisition of foreign intelligence by the directives Yahoo challenges. This acquisition is consistent with the Fourth Amendment rights of U.S. persons who are targets or whose communications are incidentally collected in the course of targeting persons abroad. ~~(S)~~

A. The Government is not required to obtain a warrant to acquire foreign intelligence information under the challenged directives. (U)

Under the Fourth Amendment's "special needs" doctrine, there is an exception to the warrant requirement where the application of the requirement would be impracticable and the search is intended to serve governmental objectives other than ordinary crime control. The purpose of foreign intelligence surveillance is, for example, to protect against terrorist attacks and other external threats, and requiring a warrant in this context would be highly burdensome. Accordingly, and as every appellate court to decide the question has held, surveillance to obtain

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

foreign intelligence information is a “special need” for which no warrant is required. (U)

Yahoo argues that the exception does not apply because obtaining foreign intelligence information need only be a “significant purpose” of an acquisition under the challenged directives. But this Court in In re Sealed Case explicitly endorsed the “significant purpose” standard, which Congress subsequently incorporated in the Protect America Act. (S)

B. Acquisition of information under the challenged directives is reasonable under the Fourth Amendment. (S)

As Yahoo acknowledges, the Government has a compelling interest in obtaining foreign intelligence information to protect the national security. Balanced against this interest are the privacy interests of U.S. persons whose communications are acquired, but those interests are amply protected by stringent safeguards the Government employs in implementing the collection. Under the challenged directives, the Government may target a U.S. person only if the Attorney General determines that there is probable cause to believe the person is a foreign power or agent of a foreign power. In addition, surveillance is authorized only for 90-day periods. These procedures are similar to requirements that this Court has held meet the Fourth Amendment test of reasonableness, and to the

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

procedures that the Government has used for decades in conducting warrantless surveillance of U.S. persons abroad outside of FISA. (S)

In addition, the DNI and the Attorney General must certify that targeting and minimization procedures are in place to protect the privacy of U.S. persons. The targeting procedures help to ensure that surveillance is reasonably believed to be limited to persons outside the United States. The minimization procedures serve to limit the acquisition, retention, and dissemination of information about U.S. persons and have also been used for decades in the context of foreign intelligence surveillance to protect the privacy interests of U.S. persons. In light of these and other safeguards employed by the Government, it is clear that the acquisition of information under the directives is constitutionally reasonable. (S)

Yahoo unpersuasively argues that acquisitions under the directives are per se unreasonable because they lack two aspects: prior judicial approval and a particularity showing. Fourth Amendment reasonableness turns on the facts and circumstances of each case, however, not on the talismanic invocation of certain factors. Numerous courts have upheld warrantless searches for foreign intelligence, and this Court should reject Yahoo's attempt to impose a back-door warrant requirement in contravention of the foreign intelligence exception. Reasonableness of foreign intelligence surveillance directed outside the United States without prior judicial approval is also supported by the fact that it is the

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Executive's longstanding practice, with the knowledge of Congress, to conduct such surveillance. (S)

Yahoo fares no better in arguing that the acquisitions are constitutionally unreasonable because the Government is not required to make a particularized showing that a targeted facility is used by a foreign power or its agent. Again, Yahoo attempts to impose the characteristics of a warrant on warrantless surveillance. [REDACTED]

[REDACTED]

[REDACTED]

(S)

Finally, and contrary to Yahoo's assertion, it is well established that the incidental collection of communications of U.S. persons during an otherwise lawful surveillance does not render the surveillance constitutionally unreasonable. That conclusion is particularly appropriate here, where the Government employs extensive minimization procedures to safeguard the privacy interests of U.S. persons. (S)

II. Yahoo may not challenge the directives on the ground that they violate the Fourth Amendment rights of third parties. (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Fourth Amendment rights are personal rights that may not be vicariously asserted, and a civil litigant may not challenge government action on the grounds that it violates the Fourth Amendment rights of others. As a matter of prudential standing, furthermore, a litigant generally must raise his own rights and not those of third parties. (U)

The FISC held that 50 U.S.C. § 1805B(g), which requires a determination whether a directive “is otherwise lawful,” eliminates prudential limitations on third-party standing. Neither the text of that provision nor its legislative history shows that Congress intended to do away with established limits on judicial review. Furthermore, that provision does not expand Yahoo’s rights under the Fourth Amendment. Yahoo’s lack of prudential standing, and absence of any protected interest under the Fourth Amendment, provide alternate grounds on which to affirm the order of the FISC. (S)

ARGUMENT (U)

I. THE ACQUISITION OF FOREIGN INTELLIGENCE INFORMATION UNDER THE CHALLENGED DIRECTIVES IS LAWFUL UNDER THE FOURTH AMENDMENT (S)

Yahoo concedes, as it must, that the Fourth Amendment is inapplicable to the vast majority of persons targeted for collection under the challenged directives—non-U.S. persons reasonably believed to be outside the United States. See Yahoo Opp. to Mot. to Compel 6 n.7, J.A. 38; United States v. Verdugo-

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Urquidez, 494 U.S. 259, 271 (1990). Accordingly, Yahoo's constitutional challenge focuses on the two categories of U.S. persons⁴ whose communications are potentially implicated by the directives: [REDACTED] U.S. persons overseas who are targeted for collection;⁵ and the U.S. persons whose communications are collected incidentally by the Government while targeting individuals abroad.⁶ (S)

The acquisition of foreign intelligence information under the challenged directives—which is accompanied by numerous and substantial procedures and safeguards to ensure that the Government's collection is limited to its purpose and to protect the privacy of U.S. persons whose communications may be collected—does not violate the Fourth Amendment rights of these U.S. persons. There is

⁴ For the purposes of this brief, the term "U.S. persons" is defined as provided in DoD Procedures and includes principally U.S. citizens and permanent resident aliens of the United States. See DoD Proc. Appx. A, 7, E.A. 400-01. (U)

[REDACTED]

⁶ In analyzing the Fourth Amendment issue in this case, the Government notes that, for at least some of the electronic communications at issue, there remains an open question whether an individual has a reasonable expectation of privacy. Nevertheless, because some courts have suggested that an individual would have a reasonable expectation of privacy in the contents of certain electronic communications while those communications are being transmitted, we assume, consistent with the position that the Government has taken before the FISC, that some acquisitions under the challenged directives implicate a reasonable expectation of privacy of at least some U.S. persons. (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

accordingly no basis for this Court to override the judgment of the Executive Branch and Congress—and endorsed by the FISC—on the appropriate balance to be struck between the Government’s foreign intelligence needs and protection of the privacy of U.S. persons. (S)

A. The Fourth Amendment’s Warrant Requirement Does Not Apply to the Collection of Foreign Intelligence Information Under the Challenged Directives. (S)

1. A Judicial Warrant Is Not Required For the Collection of Foreign Intelligence Information. (U)

The Supreme Court has recognized exceptions to the Fourth Amendment’s warrant requirement “when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.” Griffin v. Wisconsin, 483 U.S. 868, 873 (1987) (internal citations omitted); see also Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995). As this Court has recognized, every court of appeals to decide the issue has held that the Government’s need for foreign intelligence information is just such a special need, justifying an exception to the warrant requirement. See In re Sealed Case, 310 F.3d at 742 (“[A]ll the . . . courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information.”). (U)

In evaluating whether the “special needs” doctrine applies, the Supreme Court has distinguished between searches designed to uncover evidence of

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

“ordinary criminal wrongdoing” and searches that are motivated “at [a] programmatic level” by other governmental objectives. City of Indianapolis v. Edmond, 531 U.S. 32, 37-40, 48 (2001) (reviewing cases). Accordingly, the Court has permitted, inter alia, warrantless stops of motorists at roadblocks for the purpose of securing the border, see United States v. Martinez-Fuerte, 428 U.S. 543 (1976), warrantless searches of the homes of persons on probation to ensure compliance with probation conditions, see Griffin, 483 U.S. at 872, and warrantless searches of public school students in order to enforce school rules, see New Jersey v. T.L.O., 469 U.S. 325, 340 (1985).⁷ In each case, the Court concluded that the Government’s conduct of the search was motivated by a purpose that was distinct from ordinary law enforcement and difficult to reconcile with the requirement of a warrant. (U)

The same considerations apply to the Government’s conduct of a search to obtain foreign intelligence information. As this Court recognized in In re Sealed Case, the Government’s “programmatic purpose” in obtaining foreign intelligence information is “to protect the nation against terrorists and espionage threats

⁷ The Court has also approved warrantless and suspicionless drug testing of students involved in extracurricular activities, see Board of Educ. v. Earls, 536 U.S. 822, 829-38 (2002), and school athletics, see Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995); federal employees charged with enforcing drug laws or carrying firearms, see National Treasury Employees Union v. Von Raab, 489 U.S. 656, 679 (1989); and railroad employees whose job functions implicate safety concerns, see Skinner v. Railway Labor Executives’ Ass’n, 489 U.S. 602, 620 (1989). (U)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

directed by foreign powers”—a “special need” that is fundamentally different from “ordinary crime control.” In re Sealed Case, 310 F.3d at 745-46; see also Cassidy v. Chertoff, 471 F.3d 67, 82 (2d Cir. 2006) (“[T]he prevention of terrorist attacks . . . constitutes a ‘special need,’ [because] [p]reventing or deterring large-scale terrorist attacks present problems that are distinct from standard law enforcement needs and indeed go well beyond them[.]”); see also MacWade v. Kelly, 460 F.3d 260, 271 (2d Cir. 2006) (“[P]reventing a terrorist from bombing the subways constitutes a special need that is distinct from ordinary post hoc criminal investigation[.]”). (U)

Equally clearly, “the imposition of a warrant requirement [would] be a disproportionate and perhaps even disabling burden” on the Government’s ability to obtain foreign intelligence information effectively. Bin Laden, 126 F. Supp. 2d at 273. As the Fourth Circuit has explained, “attempts to counter foreign threats to the national security require utmost stealth, speed, and secrecy”; accordingly, “a warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, in some cases delay executive response to foreign intelligence threats, and increase the chance of leaks regarding sensitive executive operations.” United States v. Truong Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980) (“Truong”).⁸ (U)

⁸ While FISA addressed some of these concerns when it was passed in 1978,

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

For these reasons, every court of appeals to decide the question has held that the Government is not required, under the Fourth Amendment, to obtain a judicial warrant before conducting a foreign intelligence search. See In re Sealed Case, 310 F.3d at 742; Truong, 629 F.2d at 912-13 (upholding warrantless foreign intelligence surveillance authorized by the Attorney General); United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977) (“Foreign security wiretaps are a recognized exception to the general warrant requirement.”); United States v. Butenko, 494 F.2d 593, 605 (3d Cir. 1974) (upholding warrantless foreign intelligence surveillance); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973) (holding that “the President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence”). The holding of these cases—that the Fourth Amendment’s warrant requirement is inapplicable to the

changes in technology and the manner of collecting foreign intelligence information, as well as the increasing threat posed by transnational actors [REDACTED] make it impracticable for the Government to obtain traditional warrant or FISA court orders for the acquisitions covered by the directives. As the DNI noted in his declaration, the “process of compiling the facts necessary . . . and preparing the necessary applications [to secure authorization to conduct electronic surveillance under FISA] takes time and results in delays,” which can be exceedingly costly in the foreign intelligence context. E.A. 390. Indeed, Congress passed the Protect America Act precisely because the burden of preparing FISA applications was harming the Government’s ability to collect foreign intelligence information from targets overseas. See 153 Cong. Rec. S10,857 (Aug. 3, 2007) (remarks of Sen. McConnell) (stating that the legislation’s purpose is to provide the Government with “the speed and the flexibility” to “collect foreign intelligence concerning foreign targets overseas in another country”). (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

collection of foreign intelligence information from persons inside the United States, with appropriate approval—applies a fortiori to acquisitions, such as those at issue here, directed at persons the Government reasonably believes to be outside the United States. (S)

Furthermore, and as the FISC noted, this Court itself recognized the existence of the foreign intelligence exception to the warrant requirement in In re Sealed Case. See J.A. 176 (citing In re Sealed Case, 310 F.3d at 741-46). In In re Sealed Case, this Court held that surveillance for foreign intelligence information under FISA complied with the Fourth Amendment without determining whether an electronic surveillance order under 50 U.S.C. § 1805 constituted a “warrant” within the meaning of the Warrant Clause. See 310 F.3d at 742. As the FISC explained, “[I]f the Warrant Clause of the Fourth Amendment had been deemed applicable [in In re Sealed Case], it would have been necessary for the FISC to decide whether a FISC electronic surveillance order constituted a ‘warrant’ under the Fourth Amendment.” J.A. 176. That this Court did not undertake that analysis necessarily means that it concluded that the Fourth Amendment did not require the Government to obtain a warrant prior to conducting electronic surveillance to obtain foreign intelligence information—a conclusion that governs this case. (S)

United States v. United States District Court (Keith), 407 U.S. 297 (1972), which expressly reserved the issue of a warrant requirement for foreign

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

intelligence collection, is not to the contrary. As this Court recognized in In re Sealed Case, the Supreme Court explained in Keith “that the focus of security surveillance ‘may be less precise than that directed against more conventional types of crime’ even in the area of domestic threats to national security.” 310 F.3d at 738 (emphasis in original). The same rationale “applies a fortiori to foreign threats,” a fact that Congress necessarily recognized in passing FISA. Id.; see also Truong, 629 F.2d at 913 (“For several reasons, the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would, following Keith, ‘unduly frustrate’ the President in carrying out his foreign affairs responsibilities.”).⁹ (U)

2. The Acquisition of Foreign Intelligence Information Under the Directives Falls Squarely Within the Foreign Intelligence Exception to the Warrant Requirement. ~~(S)~~

The acquisition of information under the challenged directives falls squarely within the foreign intelligence exception to the warrant requirement. ~~(S)~~

As the Supreme Court explained in Edmond, and this Court reiterated in In re Sealed Case, the critical determinant in evaluating whether a Government activity falls under the Supreme Court’s “special needs” doctrine is the

⁹ The single case Yahoo cites in support of its position, Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975), merely “suggested the contrary in dicta, it did not decide the issue.” In re Sealed Case, 310 F.3d at 742 n.26. That dicta cannot override the uniform holdings of the courts that have actually decided the issue. ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

“programmatic purpose” of the search being challenged. 310 F.3d at 745; see also Edmond, 531 U.S. at 43 (whether a “regime of suspicionless searches” constitutes a “special need” depends on “the nature of the public interests that such a regime is principally designed to serve”). The “programmatic purpose” of the collection at issue in this case is essentially the same as in In re Sealed Case: “to protect the nation against terrorists and espionage threats directed by foreign powers.” 310 F.3d at 746. (S)

Here, as in In re Sealed Case, the Attorney General and DNI have jointly certified that a “significant purpose of the acquisition [required by each of the directives] is to obtain foreign intelligence information.” See 50 U.S.C. § 1805B(a)(4); E.A. 5, 39, 87, 141, 188, 226 . In addition, the certifications permit the acquisition of information from targeted U.S. persons only when the Government reasonably believes that those persons are outside the United States and the Attorney General determines that they are foreign powers or agents of a foreign power under section 2.5 of Executive Order 12333. [REDACTED]

[REDACTED]

DIRNSA Decl. 4-5, E.A. 11-12. Taken together, these safeguards make clear that the directives are “principally designed” to enable the government to obtain foreign

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

intelligence information, not to assist in ordinary law enforcement activities. See Edmond, 531 U.S. at 43; see also Bin Laden, 126 F. Supp. 2d at 271-77 (holding that foreign intelligence surveillance pursuant to a section 2.5 determination by the Attorney General falls within exception to the warrant requirement). ~~(TS//SI//NF)~~

Yahoo argues that foreign intelligence collection under the Protect America Act is not exempt from the warrant requirement because the Attorney General and the DNI have merely certified that obtaining foreign intelligence information is a “significant purpose” of the acquisition, not its “primary purpose.” Yahoo Br. 37-39. This argument misconceives this Court’s holding in In re Sealed Case and ignores the importance of that decision for the Government’s collection under the Protect America Act. ~~(S)~~

In In re Sealed Case, this Court read FISA’s “significant purpose” requirement to preclude “the government [from having] a primary objective of prosecuting an agent for a non-foreign intelligence crime,” and to prevent the FISA process from being “used as a device to investigate wholly unrelated ordinary crimes.” 310 F.3d at 736. As construed in this manner, this Court had no trouble concluding that the “programmatic purpose” of surveillance under FISA was distinct from ordinary law enforcement, notwithstanding that the plain language of the statute required only that the Government certify that obtaining foreign

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

intelligence information was a “significant purpose” of its acquisition. Id. at 745-46. (S)

That holding is critical here because Congress adopted the same “significant purpose” requirement in the Protect America Act, clearly intending to incorporate in the Protect America Act the same construction of that statutory requirement that this Court adopted in In re Sealed Case. See Cannon v. Univ. of Chicago, 441 U.S. 677, 696-99 (1979) (when Congress enacts statutory language identical to other statutory provisions, “it is not only appropriate but also realistic to presume that Congress was thoroughly familiar with . . . important precedents” construing that language and “it expected its enactment to be interpreted in conformity with [them]”). Accordingly, just as under traditional FISA, the Government’s primary purpose in conducting acquisitions under the Protect America Act cannot be to gather information to prosecute ordinary crimes “wholly unrelated” to foreign intelligence crimes—a limitation that further compels the conclusion that the directives are principally designed to acquire information in support of foreign intelligence activities, well beyond the needs of ordinary law enforcement. See In re Sealed Case, 310 F.3d at 736, 746. (S)

Yahoo also argues that, in determining whether a warrant is constitutionally required, this Court should ignore the requirement in the certifications underlying the directives that the Attorney General make a probable cause determination that a

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

U.S. person is an agent of a foreign power, since that requirement is not imposed by the Protect America Act. Yahoo Br. 42-44. But the question whether a particular search falls within the “special needs” exception to the Warrant Clause necessarily turns on all the facts and circumstances that relate to whether the search serves a special governmental need for which the requirement of a warrant would be impracticable—not merely those conditions that are imposed by statute. See Von Raab, 489 U.S. at 661 n.1. For example, in Von Raab, in evaluating whether the Government needed to obtain a judicial warrant before conducting employee drug testing, the Supreme Court looked not just to the bare terms of the statute governing the testing, but also to the administrative regulations implementing the statute. Id. Likewise here, the Court must look not merely to the terms of the Protect America Act but also to the procedures the Government has adopted in implementing the statute.¹⁰ (S)

¹⁰ Yahoo also contends that the Court should disregard the Attorney General’s probable cause determination under section 2.5 because, unlike FISA, regulations implementing Executive Order 12333 define the phrase “agent of a foreign power” to include employees and officers of a foreign power. See Yahoo Br. 40. Yet, as the FISC held, this distinction makes no difference to the constitutional question of whether the search in question qualifies for the foreign intelligence exception to the warrant requirement. J.A. 186; E.A. 346. In both cases, the probable cause determination affirms that the Government’s purpose in conducting the search is to gain foreign intelligence information—not to support general law enforcement activities. There is no doubt that an employee or officer of a foreign power can be a source of valuable foreign intelligence information. (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Yahoo's attempt to recast its argument as a "facial challenge" to the Protect America Act does not alter this analysis. As the FISC well understood, the scope of judicial review under section 1805B(g) is limited to determining whether a "directive was issued in accordance with subsection (e) and is otherwise lawful," 50 U.S.C. § 1805B(g) (emphasis added); it does not extend to determining whether hypothetical directives, not issued by the Government, might violate the Constitution. J.A. 181-82; E.A. 341-42. The mere fact that the Protect America Act might be (but has not been) implemented in a manner that raises constitutional concerns does not establish a valid facial challenge. See Vernonia Sch. Dist., 515 U.S. at 660; United States v. Posey, 864 F.2d 1487, 1491 (9th Cir. 1989) (rejecting litigant's attempt to challenge lawfulness of surveillance conducted under FISA on basis that "some possible applications of the FISA might violate the Fourth Amendment") (emphasis in original).¹¹ (S)

¹¹ Even assuming a facial challenge were cognizable under the Protect America Act, it would clearly fail. To prevail on its facial challenge, Yahoo must show that the Protect America Act "is unconstitutional in all its applications" or, at the very least, has no "plainly legitimate sweep." Wash. State Grange v. Wash. State Republican Party, 128 S. Ct. 1184, 1190-91 (2008). Yahoo concedes, however, that the vast majority of the Government's collection under the directives involves communications between non-U.S. persons outside the United States, to whom the Fourth Amendment does not apply. J.A. 38 n.7. (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

B. The Government's Collection of Foreign Intelligence Information Pursuant to the Directives Is Reasonable Under The Fourth Amendment. (S)

In evaluating the constitutional reasonableness of a government search, a court must look to the totality of the circumstances, United States v. Knights, 534 U.S. 112, 118 (2001), "balancing [the individual's] Fourth Amendment interests against [the search's] promotion of legitimate governmental interests," see Skinner, 489 U.S. at 619. The FISC thoroughly evaluated the circumstances surrounding the Government's acquisition of foreign intelligence information under the challenged directives and, applying this Court's holding and analysis in In re Sealed Case, correctly held that such acquisitions satisfy the Fourth Amendment reasonableness standard. J.A. 187-216; E.A. 347-76. (S)

1. Acquisitions Under the Directives Advance the Government's Compelling Interest in Obtaining Foreign Intelligence Information To Protect National Security. (S)

The Government's interest in obtaining foreign intelligence information in order to protect national security and to conduct the Nation's foreign affairs is paramount. "[I]t is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation." Haig v. Agee, 453 U.S. 280, 307 (1981) (internal citations omitted). The terrorist threat at issue here "may well involve the most serious threat our country faces." In re Sealed Case, 310 F.3d at 746. The collection of foreign intelligence information from Yahoo, [REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED] See supra pp. 13-14; [REDACTED] Decl. 2, E.A. 274. Thus, as the FISC recognized, there is “little doubt about the weightiness of the government’s interest” in this case. J.A. 187; see also Yahoo FISC Stay Mot. 16 (“Yahoo! does not dispute that the government has a compelling interest in obtaining foreign intelligence information to protect national security.”). (S)

2. **The Privacy Interests of U.S. Persons Are Protected by Stringent Safeguards and Procedures.** (S)

[REDACTED]

[REDACTED] the only constitutional interests at stake are those of [REDACTED]

[REDACTED] U.S. persons targeted for surveillance, see DNI Decl. 15, E.A. 391

[REDACTED]

[REDACTED] and U.S.

persons whose communications are incidentally collected in the course of targeting another person outside the United States. The Government employs multiple safeguards that are designed to ensure that surveillance is appropriately targeted at individuals outside the United States for foreign intelligence purposes and to protect the privacy interests of [REDACTED] U.S. persons targeted abroad and other U.S. persons who communicate with targets. These safeguards and procedures—many of which provide protections well beyond what courts have held reasonable in the context of warrantless searches involving less compelling

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

governmental interests¹²—adequately protect the privacy interests of U.S. persons.

~~(S)~~

a. The Attorney General must make a probable cause determination Under E.O. 12333. ~~(S)~~

Before the Government targets a U.S. person under the directives, the Attorney General must have authorized the acquisition pursuant to section 2.5 of Executive Order 12333, which requires the Attorney General to determine that there is probable cause to believe that the targeted U.S. person is a foreign power or an agent of a foreign power. E.A. 5, 39, 87, 141-42, 188, 226; see also DoD Proc. Annex 2-3, E.A. 395-96 (defining the term “agent of a foreign power”). ~~(S)~~

To ensure that the Attorney General is able to make an informed judgment that the U.S. person meets this definition, applicable procedures require the Government to compile an application for the Attorney General that includes: (1) an identification or description of the target; (2) a statement of facts supporting findings that (a) there is probable cause to believe that the target is a foreign power or an agent of a foreign power; (b) the acquisition is necessary to obtain significant foreign intelligence or counterintelligence; and (c) the intelligence expected to be obtained could not reasonably be obtained by other less intrusive means; (3) a description of the significant foreign intelligence or counterintelligence expected to

¹² See supra pp. 23-24 and note 7. (U)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

be obtained; (4) a statement of period of time, not to exceed 90 days, for which the surveillance is required; and (5) a description of the procedures governing the retention and dissemination of incidentally acquired communications. See DoD Procedures, Proc. 5, Pt. 2.C, J.A. 61-62. (S)

The Attorney General's probable cause determinations for the directives are similar to the determinations that the Attorney General and the FISC must make under the electronic surveillance and physical search provisions of FISA, see 50 U.S.C. §§ 1804-1805, 1823-1824, which this Court has held satisfy the Fourth Amendment's central requirement of reasonableness. See In re Sealed Case, 310 F.3d at 739; see also Bin Laden, 126 F. Supp. 2d at 279 & n.18. Moreover, as the FISC noted, the determination must be renewed every 90 days, the exact same length of time that this Court found reasonable in In re Sealed Case, 310 F.3d at 740. J.A. 207-08. Furthermore, the procedures employed under section 2.5 of Executive Order 12333 are the same procedures that for over 25 years have governed the warrantless surveillance of U.S. persons abroad outside the context of FISA.¹³ (S)

¹³ If this Court were to determine that these procedures are insufficient to render reasonable the collection of communications of U.S. persons under the Protect America Act, its decision could thus also raise serious questions about the Government's decades-long collection for foreign intelligence purposes of communications that do not fall within the ambit of FISA. (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

When Congress initially enacted FISA in 1978, it was “[w]ithout question . . . aware” of the warrantless surveillance of U.S. persons outside the United States and chose to “exclude[] overseas surveillance from the statute,” J.A. 201, including a substantial amount of such surveillance conducted inside the United States. This decades-long practice of conducting warrantless foreign intelligence surveillance on U.S. persons manifests the understanding of both the Executive and Legislative Branches, endorsed repeatedly by courts, 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,” J.A. 201-02, E.A. 361-62, and that the procedures employed under section 2.5 adequately protect the interests of U.S. persons. Such long-standing congressional acquiescence in Executive practice is entitled to great weight, particularly in the realm of foreign affairs. See, e.g., Dames & Moore v. Regan, 453 U.S. 654, 686 (1981). (S)

b. Senior officials certify that the Government’s procedures satisfy statutory requirements. (S)

The Protect America Act also requires the DNI and the Attorney General to certify that procedures are in place to protect the privacy of U.S. persons, including targeting procedures and minimization procedures. 50 U.S.C. § 1805B(a)(1), (5). In addition, the DNI and the Attorney General must also certify that a significant purpose of the acquisition is to obtain foreign intelligence information. See id. §

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

1805B(a). As the FISC recognized, the requirement that these senior Executive officials themselves certify that the procedures comply with statutory requirements of the Protect America Act “represent[s] a sufficient restraint on the exercise of arbitrary action by those in the executive branch who are effecting the actual acquisition of information.” J.A. 209. See also In re Sealed Case, 310 F.3d at 739 (recognizing the importance of such “internal check[s] on Executive Branch arbitrariness”) (internal citations omitted). (S)

c. Targeting procedures ensure that the Government targets only persons reasonably believed to be outside the United States. (S)

The targeting procedures employed by the Government—which the FISC upheld, E.A. 571—serve to ensure that only persons reasonably believed to be located outside the United States are surveilled. See 50 U.S.C. § 1805B(a)(1). Under these procedures, once the Government has reason to believe that the surveillance of the target may generate foreign intelligence information, it considers a range of information in determining whether the target is reasonably believed to be outside the United States. See, e.g., E.A. 14-17. The Government also may [REDACTED]

[REDACTED] See, e.g., E.A. 14-16. (S)

After initiating surveillance, the Government conducts [REDACTED] analyses to “detect those occasions when a person who when targeted was

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

reasonably believed to be located overseas has since entered the United States,” in which case acquisition must be “terminated without delay.” See, e.g., E.A. 16-17. If information is mistakenly acquired from a target inside the United States, the information attributable must be purged from Government databases (with limited exceptions) and the incident must be reported to the Department of Justice and the Office of the Director of National Intelligence. See, e.g., E.A. 19. ~~(S)~~

d. Minimization procedures protect the privacy of U.S. persons whose communications are acquired. ~~(S)~~

The Protect America Act further requires the Government to employ minimization procedures, as defined in FISA, to limit the acquisition, retention, and dissemination of information concerning U.S. persons. See 50 U.S.C. § 1805B(a)(5); see also id. § 1801(h). The Government’s minimization procedures require, among other things, that the identity of U.S. persons be redacted from intelligence reports prior to dissemination unless the information constitutes foreign intelligence information, is necessary to understand foreign intelligence information, or is evidence of a crime. See, e.g., E.A. 534-36. The FISC correctly recognized that the minimization procedures are virtually identical to those used by the FISC in traditional FISA surveillance, and are “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 Yahoo.” J.A. 206-07. Indeed, this Court cited the use of such minimization


~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

procedures in In re Sealed Case as an important factor in holding traditional FISA surveillance to be reasonable under the Fourth Amendment. In re Sealed Case, 310 F.3d at 740. (S)

- e. **A significant purpose of the acquisition must be to obtain foreign intelligence information.** (S)

The Protect America Act also mandates that acquisitions be undertaken only if a “significant purpose” is to “obtain foreign intelligence information.” 50 U.S.C. § 1805B(a)(4). The requirement, as we have explained, precludes the Government from using directives issued under the Protect America Act “as a device to investigate wholly unrelated ordinary crimes.” In re Sealed Case, 310 F.3d at 736.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~J.A. 211; E.A. 37.¹⁴~~(TS//SI//NF)~~

3. **The Absence of Other Factors Does Not Render the Acquisitions Unreasonable.** ~~(S)~~

Yahoo nevertheless argues that the absence of two specific factors—prior judicial approval and a finding of particularity that the targeted facility is being used by the target—renders the directives per se unreasonable under the Fourth Amendment. See Yahoo Br. 46 (arguing that these factors are “constitutionally required” under In re Sealed Case). ~~(S)~~

This argument fundamentally misconstrues the reasonableness standard that is the hallmark of the Fourth Amendment. As the Supreme Court has often explained, the determination whether a search is reasonable “requires careful attention to the facts and circumstances of each particular case.” Graham v. Connor, 490 U.S. 386, 396 (1989). Accordingly, “[n]o one factor can be a talismanic indicator of reasonableness.” United States v. Redmon, 138 F.3d 1109, 1128 (7th Cir. 1998). (U)

Consistent with these principles, In re Sealed Case did not purport to set in stone a list of factors that must be present for a court to determine that the

¹⁴ The Protect America Act also contains oversight, reporting, and sunset provisions, like those considered by this Court with respect to traditional FISA in In re Sealed Case. See 310 F.3d at 741 n.25; 50 U.S.C. § 1805B(d); 121 Stat. 552 §§ 4, 6(c). (U)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Government's foreign intelligence surveillance is reasonable under the Fourth Amendment. To the contrary, it expressly acknowledged that the procedures it considered in evaluating the reasonableness of FISA surveillance—procedures required by Title III for ordinary criminal warrants—were “not constitutionally required.” In re Sealed Case, 310 F.3d at 737 (emphasis added).¹⁵ The Court looked instead to such procedures as “instructive” to its reasonableness analysis, recognizing—as the FISC did below—that reasonableness depends on the “facts and circumstances of each case.” Id. at 737, 740. Applying this same standard here, it is apparent that neither of the factors identified by Yahoo renders the acquisitions at issue unreasonable. (S)

a. Prior court approval for each target is not required.
(S)

Yahoo first argues that, in order for the acquisitions under the directives to be reasonable, the Government must obtain prior judicial approval of its probable cause determination that a U.S. person targeted for collection is an agent of a foreign power. This contention amounts to nothing more than an attempt to impose a back-door warrant requirement on foreign intelligence surveillance that,

¹⁵ Given FISA's resemblance to a traditional warrant regime, it made sense for this Court in In re Sealed Case to compare it to the Title III procedures in assessing reasonableness. See 310 F.3d at 737-742. But the Court by no means held that such procedures were constitutionally required and simply weighed such factors, among many others, in its assessment of the reasonableness of the FISA court orders under the Fourth Amendment. See id. (U)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

as we have explained, is exempt from just such a requirement.¹⁶ The Supreme Court has expressly held that, where it is impracticable to obtain a warrant upon a showing of probable cause to believe that a crime has been committed, as is the case here, the Fourth Amendment may not be construed to require prior judicial approval based on some lesser showing. See Griffin, 483 U.S. at 877. As the Griffin Court explained, requiring prior judicial approval and a showing other than criminal probable cause—as Yahoo would here—is “a combination that neither the text of the Constitution nor any of our prior decisions permits.” Id. (S)

Yahoo is mistaken in arguing that the FISC “departed dramatically” from In re Sealed Case by holding acquisition under the directives to be reasonable in the absence of prior judicial approval for each Government target. As the opinion below makes plain, the FISC faithfully recounted and carefully applied this Court’s prior holding. J.A. 190-211; E.A. 350-71. The FISC recognized, however, that the circumstances of the acquisition in this case differ significantly from those at issue in In re Sealed Case, and that the Government was not bound to employ the same protections here that this Court held to be reasonable in that case. In particular, the

¹⁶ Yahoo effectively concedes as much by arguing that reasonableness must be assessed in relation to the requirements for a warrant. See Yahoo Br. 50. Not surprisingly, the cases that Yahoo cites for this proposition involved circumstances that, unlike the foreign intelligence acquisitions here, were found to require a warrant in the first place. See Keith, 407 U.S. at 323-24; Coolidge v. New Hampshire, 403 U.S. 443, 472 (1971). (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Court noted that the acquisition at issue here is directed exclusively at persons outside the United States, while In re Sealed Case involved the surveillance of United States persons located within the United States. Because surveillance of persons outside the United States is far less likely to implicate rights protected by the Fourth Amendment, that difference alone significantly diminishes the privacy interests involved and shifts the constitutional balance in favor of the Government. J.A. 200-02; E.A. 360-62 (discussing the Bin Laden court's holding that prior judicial review is not required for a search of a United States person outside the United States). That the correct constitutional balance is struck by the directives is particularly true in light of the fact that a probable cause determination is made by the Attorney General when a U.S. person is targeted. Tellingly, Yahoo does not cite a single case holding that prior judicial approval is a necessary element of reasonableness in the context of foreign intelligence surveillance targeting individuals located outside the United States. ~~(S)~~

In addition to being inconsistent with Fourth Amendment principles, Yahoo's per se requirement of prior judicial approval would also upend the Government's long-standing practice, recognized by Congress, of conducting surveillance directed at persons outside the United States without obtaining a warrant. J.A. 201; supra p. 7-8. Although, as we have explained, FISA's coverage expanded over time due to technological advances, see supra pp. 8-9, at the time of

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

its enactment, FISA did not regulate most acquisitions conducted in the United States of foreign and international communications. Congress enacted the Protect America Act for the express purpose of again exempting surveillance targeting individuals located abroad from FISA's requirement of prior judicial review—whether or not the surveillance itself takes place inside the country. See supra pp. 9-10. Thus, notwithstanding Yahoo's claim to the contrary, see Yahoo Br. 52-53, the historical practice of both the Executive Branch and Congress strongly supports the conclusion that prior judicial approval is not required for surveillance targeting persons outside the country, even where as here the acquisitions themselves occur inside the country.¹⁷ This considered practice is, of course, entitled to significant deference. (S)

b. The methods used to identify the facilities to be targeted are reasonable. (S)

Yahoo also contends that acquisitions under the directives are unreasonable because the Protect America Act does not require the Government to establish probable cause that a particular facility (e.g., a particular e-mail address) is being used or is about to be used by a foreign power or its agent. See Yahoo Br. 53-58. Once again, however, Yahoo conflates the test for constitutional reasonableness

¹⁷ Notably, the fact that communications between foreign persons located outside the United States happen to be intercepted on U.S. soil does not mean that they are protected by the Fourth Amendment, as the FISC correctly recognized, J.A. 205, and Yahoo does not dispute. (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

with the different requirements for a warrant under the Fourth Amendment. See U.S. Const. amend. IV (“no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched”) (emphasis added).¹⁸ Although particularity may be considered as one factor among many in assessing the overall reasonableness of particular search, “the Fourth Amendment imposes no irreducible requirement” of individualized findings where the search in question is otherwise reasonable, as it is here. Martinez-Fuerte, 428 U.S. at 561. (S)

In all events, and contrary to Yahoo’s claims, the Government employs extensive procedures to ensure that the specific facilities selected for collection are connected to persons who may be targeted under the Protect America Act. [REDACTED]

[REDACTED]

¹⁸ Yahoo’s reliance on Berger v. New York, 388 U.S. 41, 56 (1967), and United States v. Carter, 413 F.3d 712, 715 (8th Cir. 2005), which discuss particularity requirements for a warrant, reflects this misunderstanding of the Fourth Amendment. See Yahoo Brief at 55-57. (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Further, the Government conducts [REDACTED] analyses and checks of the e-mail accounts to determine whether a person who was reasonably believed to be located overseas has since entered the United States. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Yahoo

is therefore wrong to suggest that the Government's procedures do not establish a sufficient connection between the foreign intelligence collection the Government is statutorily authorized to undertake and the targets it selects for surveillance.¹⁹

~~(S//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

As for Yahoo's speculation that confusing or mistyping a digit or character [REDACTED] is likely to result in the inadvertent targeting of a U.S. person, the risk of such clerical mistakes—which could occur just as easily after obtaining court approval under traditional FISA or Title III provisions—does not render the challenged directives unconstitutional. See Pasiewicz v. Lake County Forest Preserve Dist., 270 F.3d 520, 525 (7th Cir. 2001) (“[T]he Fourth Amendment demands reasonableness, not perfection.”). While mistakes are theoretically possible, the presumption is in favor of government regularity, not the opposite. Cf. United States Postal Serv. v. Gregory, 534 U.S. 1, 10 (2001) (noting that “a presumption of regularity attaches to the actions of Government agencies”).

~~(S)~~

4. The Incidental Collection of Communications of U.S. Persons Does Not Violate the Fourth Amendment. ~~(S)~~

Finally, while Yahoo repeatedly emphasizes the possibility that the acquisitions could inadvertently include communications of U.S. persons not targeted for surveillance, it is well established that the incidental collection of communications of U.S. persons during an otherwise lawful surveillance does not render the surveillance constitutionally unreasonable. J.A. 373-74; United States v.

[REDACTED] the account is used by a person who is reasonably believed to be located outside the United States and that a significant purpose of the acquisition is to acquire foreign intelligence information. ~~(S)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Figueroa, 757 F.2d 466, 472-73 (2d Cir. 1985); United States v. Tortorello, 480 F.2d 764, 775 (2d Cir. 1973) (holding that once the relevant authority for the search has been established as to one participant, the statements of other, incidental “participants may be intercepted if pertinent to the investigation”); see also United States v. Kahn, 415 U.S. 143, 157 (1974) (interception of wife’s communications incident to lawful wiretap of home phone targeting husband’s communications did not violate the Fourth Amendment).²⁰ Notwithstanding Yahoo’s claim to the contrary, this conclusion applies fully—if not more forcefully—to surveillance in the foreign intelligence context. See Butenko, 494 F.2d at 608 (“To be sure, in the course of such wiretapping conversations of alien officials and agents, and perhaps of American citizens, will be overheard and to that extent, their privacy infringed. But the Fourth Amendment proscribes only ‘unreasonable’ searches and seizures.”); Brown, 484 F.2d at 425; Bin Laden, 126 F. Supp. 2d at 280 (“[I]ncidental interception of a person’s conversations during an otherwise lawful surveillance is not violative of the Fourth Amendment.”). (S)

This conclusion is particularly appropriate here because the privacy interests of U.S. persons whose communications are incidentally collected are specifically

²⁰ Yahoo cannot distinguish these cases on the ground that in those cases the Government had obtained findings of criminal probable cause for the targets of the surveillance. That fact may be relevant to whether the search as a whole is reasonable, but it does nothing to alter the conclusion that an otherwise lawful surveillance does not become unlawful simply because it incidentally includes the communications of persons not targeted for surveillance. (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

protected by the minimization procedures described above. Indeed, the FISC found this fact important to its decision upholding the Government's targeting procedures under the Protect America Act. E.A. 569 n.15 (stating that, when the Government incidentally acquires U.S. person information pursuant to the Protect America Act, such information "will be afforded the protection of FISA minimization procedures"). Such a finding also comports with this Court's holding in In re Sealed Case that the use of minimization procedures supports a finding of reasonableness under the Fourth Amendment. See 310 F.3d at 740-41. See also J.A. 214-15 (holding that "these minimization procedures adequately protect the privacy interests of persons whose communications might be incidentally acquired"). And the judges of the FISC have regularly found nearly identical minimization procedures to be "reasonable under circumstances in which the government is intercepting private email communications." J.A. 206.²¹ If this Court were to hold that the Government must obtain a judicial order whenever it

²¹ Yahoo also challenges, in passing, the lack of a requirement in the Protect America Act that the Government make a "necessity" or "less intrusive means" determination before conducting surveillance of foreign intelligence targets located outside the United States. See Yahoo Br. 49, 59. Yahoo is wrong both as a legal and factual matter. Where the Government targets a U.S. person, the DoD Procedures expressly require a finding that the intelligence could not reasonably be obtained by other less intrusive techniques. See DoD Procedures, Proc. 5, Pt. 2.C.(2)(c), J.A. 62. And in any event, the Supreme Court has held that the use of least intrusive means is not a required element of reasonableness. See Illinois v. Lafayette, 462 U.S. 640, 647 (1983) ("The reasonableness of any particular governmental activity does not necessarily or invariably turn on the existence of alternative 'less intrusive' means."). (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

might incidentally acquire U.S. person communications when targeting persons overseas, it would call into question significant foreign intelligence activity that has been conducted for decades with the knowledge of Congress. (S)

* * * * *

In sum, in passing and implementing the Protect America Act, Congress and the Executive Branch acted in concert to develop a framework of specific procedures and safeguards to ensure that acquisitions under the directives only minimally implicate the privacy of U.S. persons, and then do so only in a targeted manner. That framework is entitled to the utmost constitutional respect by this Court. See Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635-37 (1952) (Jackson, J., concurring). Evaluating the totality of the circumstances and weighing the compelling governmental interests at stake in combination with the extensive safeguards the Government employs to protect the privacy interests of U.S. persons—including: (1) the probable cause requirement under section 2.5 for U.S. person targets; (2) targeting procedures to ensure that only individuals abroad are surveilled; (3) minimization procedures to protect the privacy of both U.S. person targets and U.S. persons whose communications are incidentally acquired; and (4) factors designed to ensure that foreign intelligence information is obtained—the FISC correctly held that the Government’s acquisition of foreign

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

intelligence information under the directives meets the Fourth Amendment's central requirement of reasonableness. (S)

II. YAHOO MAY NOT CHALLENGE THE DIRECTIVES ON THE BASIS THAT THEY VIOLATE THE FOURTH AMENDMENT RIGHTS OF THIRD PARTIES (S)

This Court may also affirm the FISC Order on the ground that Yahoo may not vicariously invoke the constitutional rights of third parties not before the Court, *i.e.*, U.S. persons whose communications are acquired pursuant to the directives. (S)

Yahoo's constitutional challenge rests entirely on the alleged violation of the rights of third parties, but the Supreme Court has repeatedly held that "Fourth Amendment rights are personal rights which . . . may not be vicariously asserted." Alderman v. United States, 394 U.S. 165, 174 (1969); accord Rakas v. Illinois, 439 U.S. 128, 140 (1978); Minnesota v. Carter, 525 U.S. 83, 88 (1998) (criminal defendant seeking suppression of evidence must "show the violation of his (and not someone else's) Fourth Amendment rights"). This substantive principle of Fourth Amendment law also bars a civil litigant from challenging government action on the ground that it violates the Fourth Amendment rights of others. Thus, in California Bankers Ass'n v. Schultz, 416 U.S. 21 (1974), the Supreme Court refused to consider a bank's claim that certain federal reporting requirements violated the Fourth Amendment rights of non-party bank customers "whose

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

transactions must be reported” under federal law. Id. at 69-70 & n.8. Similarly, in Hollingsworth v. Hill, 110 F.3d 733 (10th Cir. 1997), the court of appeals held that a mother could not challenge deputy sheriffs’ seizure of her minor children on the ground that it violated those children’s Fourth Amendment rights. Id. at 738; see also, e.g., Ellwest Stereo Theatres, Inc. v. Wenner, 681 F.2d 1243, 1248 (9th Cir. 1982) (rejecting adult theater’s challenge to city ordinance on ground that any police surveillance enabled by the ordinance did not threaten the theater’s Fourth Amendment interests, but only “the interests of its patrons”). (S)

Furthermore, prudential standing rules require that a party typically “must assert his own legal rights and interests, and cannot rest his claim to relief on the legal rights or interests of third parties,” even where the claims are being raised “defensively.” Warth v. Seldin, 422 U.S. 490, 499, 500 n.12 (1975); see also, e.g., Kowalski v. Tesmer, 543 U.S. 125, 128-29 (2004). Standing principles are inherent in the separation of powers, see DaimlerChrysler v. Cuno, 547 U.S. 332, 341-46 (2006), and are no less important when it comes to challenges to foreign intelligence surveillance. See ACLU v. National Security Agency, 493 F.3d 644 (6th Cir. 2007), cert. denied, 128 S. Ct. 1334 (2008). (U)

The FISC held that the general bar against invoking third-party rights did not apply because, under 50 U.S.C. § 1805B(g), the FISC reviews a directive to determine if it was “was issued in accordance with [§ 1805B(e)] and is otherwise

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

lawful”—which the FISC construed to eliminate prudential limits on third-party standing. J.A. 161-62, 165-67. But “Congress legislates against the background of [the Supreme Court’s] prudential standing doctrine, which applies unless it is expressly negated.” Bennett v. Spear, 520 U.S. 154, 163 (1997). Nothing in the phrase “is otherwise lawful” serves to “expressly negate[]” prudential limitations on third-party standing. Nor is there any indication in the legislative history of the statute that Congress intended to wipe out established limitations on judicial review. (S)

In addition, the statutory phrase “is otherwise lawful” does not modify substantive Fourth Amendment restrictions on a litigant’s ability to invoke the constitutional rights of third parties. See, e.g., California Bankers Ass’n, 416 U.S. at 69-70; Rakas, 439 U.S. at 139-42. In this regard, it is significant that a court evaluating a warrantless search under the Fourth Amendment must consider “all the facts and circumstances,” South Dakota v. Opperman, 428 U.S. 364, 375 (1976)—a task that would be difficult or even impossible in the context of a third-party challenge. (S)

Absent an explicit abrogation of prudential standing limits, there is no basis for third-party standing, which is typically limited to circumstances in which the litigant “has a ‘close’ relationship with the person who possesses the right” and “there is a ‘hindrance’ to the possessor’s ability to protect his own interests.”

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Kowalski, 543 U.S. at 130. Yahoo has no “close” relationship with the third parties whose communications might be disclosed in the course of the Government’s surveillance of foreign intelligence targets abroad. Those third parties also have other means by which to vindicate their Fourth Amendment rights, such as by challenging the lawfulness of surveillance if the Government seeks to use any evidence obtained against them in criminal proceedings.²² (S)

In sum (although it is not necessary for the Court to reach this issue to decide the case), the FISC erred in permitting Yahoo to challenge the directives on the ground that they violated the Fourth Amendment rights of third parties not before the Court. Yahoo’s lack of prudential standing, and the absence of any protected interest under the Fourth Amendment, accordingly provide alternate bases for affirming the order on appeal. (S)

CONCLUSION (U)

For all the reasons set forth herein, the judgment of the FISC should be affirmed. (S)

²² As the D.C. Circuit noted in Haitian Refugee Ctr. v. Gracey, 809 F.2d 794, 810 (D.C. Cir. 1987), cases in which courts have recognized third-party standing have typically involved constitutional rights protecting the relationship between the litigant and the third party whose rights they seek to invoke. See, e.g., Griswold v. Connecticut, 381 U.S. 479 (1965) (right to receive professional medical advice on the use of contraceptives; Pierce v. Society of Sisters, 268 U.S. 510 (1925) (right to educate child in school of parent’s choice). No comparable protected relationship is at issue here. (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Respectfully submitted,



Michael B. Mukasey
Attorney General

Mark Filip
Deputy Attorney General

J. Patrick Rowan
Acting Assistant Attorney General

John A. Eisenberg
Office of the Deputy Attorney General


Office of Legal Counsel


Civil Division

Matthew G. Olsen
John C. Demers


National Security Division

United States Department of Justice

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

CERTIFICATE OF SERVICE (U)

I hereby certify that the foregoing Brief for Respondent was served by hand-delivery on June 5, 2008, to the Litigation Security Officer, [REDACTED] or her delegate, for forwarding to the Court. A redacted copy of the brief will be served separately upon the Litigation Security Officer, or her delegate, for forwarding to counsel for Petitioner. (U)



National Security Division

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

CERTIFICATE OF COMPLIANCE (U)

Pursuant to Federal Rule of Appellate Procedure 32(a)(7)(C), I hereby certify that the Brief for Respondent complies with the type-volume limitations of Fed. R. App. P. 32(a)(7)(B) because it contains 13,342 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). The brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Times New Roman. (U)



National Security Division

~~TOP SECRET//COMINT//ORCON,NOFORN~~