~~SECRET~~

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, DC

FEB 15 PM 6:11

CLERK OF COURT

IN RE DIRECTIVES TO YAHOO INC. PURSUANT TO SECTION 105B OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT. (S)	Docket Number: 105B(g) 07-01

UNITED STATES OF AMERICA'S SUPPLEMENTAL BRIEF ON THE FOURTH AMENDMENT

Matthew G. Olsen
Deputy Assistant Attorney General

John Eisenberg
Deputy Assistant Attorney General

John C. Demers
Deputy Assistant Attorney General

[redacted]
Counsel to the Assistant Attorney General

[redacted]
Counsel to the Assistant Attorney General

Office of Legal Counsel
U.S. Department of Justice

[redacted]
Attorney Advisors
Office of Intelligence Policy and Review

[redacted]
Counsel for National Security Law & Policy
Office of Law and Policy

National Security Division
U.S. Department of Justice

~~SECRET~~

Classified by:	Matthew G. Olsen, Deputy Assistant Attorney General, NSD, DOJ
Reason:	1.4 (c)
Declassify on:	15 February 2033

INTRODUCTION (U)

Pursuant to this Court's Order of February 6, 2008, the United States of America, through the undersigned Department of Justice attorneys, submits this brief to address the question whether the directives at issue here require Yahoo! Inc. ("Yahoo") "to assist the Government in acquiring any class of communications or information in which a United States citizen would have a legitimate expectation of privacy under the Fourth Amendment."[1] Consistent with the position the Government has taken in this Court in previous filings, we answer this question in the affirmative, at least to the extent that the Government would acquire electronic communications [redacted] (S)

The existence of a reasonable expectation of privacy is, of course, the beginning, not the end, of the constitutional inquiry. Where a reasonable expectation of privacy in certain communications exists, acquisition of such communications must comply with the safeguards of the Fourth Amendment. The acquisition of at issue here readily complies with the Fourth Amendment. The Government's collection of foreign intelligence information fits comfortably within the special needs exception to the Fourth Amendment's warrant requirement. The question therefore becomes whether the acquisitions meet the Fourth Amendment's overriding requirement of reasonableness. As explained in detail in the Government's prior submissions and discussed further below, the protections and safeguards Congress and the Executive Branch have required for acquisitions under the Protect America Act are more than sufficient to make the acquisition constitutionally reasonable. (S)

[1] Consistent with the Government's prior submissions, the analysis in this brief focuses on the Fourth Amendment rights of U.S. persons, a category which includes but is not limited to U.S. citizens. See 50 U.S.C. § 1801(i). Because, in general, the Fourth Amendment rights of non-citizen U.S. persons are substantially coextensive with the rights of U.S. citizens, the analysis in this brief applies equally to U.S. citizens. See United States v. Verdugo-Urquidez, 494 U.S. 259, 265 (1990). (S)

Importantly, the Government relies on many of these same protections and safeguards to help establish the reasonableness of its long-standing collection of foreign intelligence outside FISA. For decades, the Government—with the knowledge of Congress—has conducted surveillance of foreign intelligence targets outside FISA pursuant to executive order, subject to Attorney General-approved minimization procedures and Congressional oversight. Although these collections result in the incidental acquisition of communications of U.S. persons, these long-standing practices comply with the Fourth Amendment in part because the Government has adopted stringent minimization procedures to protect the privacy interests of United States persons. A determination by this Court that the procedures at issue here do not satisfy the Fourth Amendment, at least with respect to incidental collections, would be contrary to this well-established practice and could call into question for the first time not only the acquisition contemplated by the directives at issue here but also the Government's collection of foreign intelligence under established authorities. Nothing in the Fourth Amendment requires such a conclusion. ~~(S)~~

ARGUMENT (U)

I. U.S. Persons Abroad and U.S. Persons Communicating with Foreign Intelligence Targets Have a Reasonable Expectation of Privacy in the Content of Certain Communications Acquired Pursuant to the Directives. ~~(S)~~

The directives at issue require Yahoo to assist the Government in acquiring foreign intelligence information concerning persons reasonably believed to be outside the United States. See 50 U.S.C. §§ 1805B(a), 1805B(e). The directives therefore implicate, to varying degrees, the Fourth Amendment rights of two categories of U.S. persons: (1) persons outside the United States who are the targets of an acquisition; and (2) persons, whether abroad or inside the United States, who are communicating with foreign intelligence targets outside the United States. ~~(S)~~

In both cases, the directives require Yahoo to assist the Government in acquiring certain types of communications while those communications are in transmission. See [redacted] Aff. ¶¶ 5-9 (discussing information intercepted during transmission); see also [redacted] Aff. ¶¶ 13-14 (same). Whether a person has a reasonable expectation of privacy in any particular case, of course, requires the evaluation of the specific facts presented.[2] While the general question has not been definitively resolved in the courts, the Government has argued before this Court that U.S. persons have a reasonable expectation of privacy in the content of such electronic communications, at least until they are received by their intended recipients.[3] See [redacted] On the basis of the Government's position, this Court has asserted

[2] See, e.g., United States v. Dorais, 241 F.3d 1124, 1129 (9th Cir. 2001). As a result, a user of certain Internet services, such as those provided by Yahoo, may agree to terms of service confirming the provider's authority to access information submitted to the provider or disclose such information in response to requests from the Government. Decisions in analogous contexts establish that consent to such terms can undermine any reasonable expectation of privacy under the Fourth Amendment. See United States v. Young, 350 F.3d 1302, 1308-09 (11th Cir. 2003) (terms of service giving FedEx authority to consent to package search); Muick v. Glenayre Electronics, 280 F.3d 741, 743 (7th Cir. 2002) (employer announcement that it could inspect laptops); Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) (privacy disclaimer in an electronic bulletin board); cf. United States v. Miller, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."). ~~(S)~~

[3] Any expectation of privacy that exists is limited to the content of the communications. The Supreme Court has held that persons have no reasonable expectation of privacy in dialing, routing, addressing, and signaling information that they share with communications providers. See Smith v. Maryland, 442 U.S. 735, 743-44 (1979). This holding naturally encompasses "header" information that is attached to electronic communications, identifying, inter alia, the sender of a communication, its recipient, and the time and date of its transmission. See United States v. Forrester, 495 F.3d 1041, 1048-49 (9th Cir. 2007) (holding that the surveillance of e-mail header information is "constitutionally indistinguishable from the use of a pen register that the Court approved in Smith"). ~~(S)~~

[4] The courts have generally reached the same conclusion. See, e.g., Warshak v. United States, 490 F.3d 455, 469-76 (6th Cir. 2007) (analogizing e-mails to telephone calls and holding that an individual generally has a reasonable expectation of privacy in the content of e-mails, among other things, that "are . . . sent or received through, a commercial ISP"), vacated and pet'n for reh'g en banc granted, Oct. 9, 2007; United States v. Jones, 149 Fed. Appx. 954, 959 (11th Cir. 2005) ("We have not addressed previously the existence of a legitimate expectation of privacy in text messages or e-mails. Those circuits that have addressed the question have compared e-mails with letters sent by postal mail. Although letters are protected by the Fourth Amendment, 'if a letter is sent to another, the sender's expectation of privacy ordinarily terminates upon delivery.'") (quoting United States v. King, 55 F.3d

jurisdiction and granted numerous orders authorizing the surveillance and search of various foreign intelligence targets. See, e.g., [redacted] Thus, [redacted], the Government does not contest that the acquisition contemplated by the directives would implicate the reasonable expectation of privacy of U.S. persons. (S)

II. The Acquisition of Foreign Intelligence Information Pursuant to The Directives Satisfies the Fourth Amendment. (S)

Because it implicates the reasonable privacy expectations of U.S. persons, the acquisition must, of course, comply with the Fourth Amendment. As the Government has already established, no warrant is required for such surveillance, and the extensive procedures and safeguards in place ensure compliance with the Fourth Amendment's fundamental requirement of reasonableness.[5] See Mem. in Support of the Government's Mot. to Compel Compliance with Directives of the Director of National Intelligence and Attorney General at 11-17, Docket No. 105B(g) 07-01 (Dec. 11, 2007) ("Gov't Mem."). (S)

A. No Warrant Is Required For Foreign Intelligence Surveillance. (S)

The Fourth Amendment does not require the Government to obtain a warrant to conduct the surveillance contemplated by the directives. Rather, because the acquisition is conducted for the purpose of obtaining foreign intelligence information, it falls within the special needs exception to the Warrant Clause. See Gov't Mem. at 8-12. (S)

1193, 1195-96 (6th Cir. 1995); United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996) ("[T]he transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant."). (S)

[5] The fact that the acquisitions authorized by the directives may implicate the Fourth Amendment rights of U.S. persons does not give Yahoo the ability vicariously to assert the Fourth Amendment rights of its customers, much less of any individual whose communications happen to pass through its servers. See Gov't Mem. at 5-7; Gov't Reply to Sur-reply at 1-4; see also California Bankers Ass'n v. Shultz, 416 U.S. 21 (1974); Ellwest Stereo Theatres, Inc. v. Wenner, 681 F.2d 1243, 1248 (9th Cir. 1982). (S)

The acquisition at issue—foreign intelligence surveillance—addresses a "special governmental need[] beyond the normal need for law enforcement," that justifies an exception to the warrant requirement of the Fourth Amendment. Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 665-66 (1989); see, e.g., MacWade v. Kelly, 460 F.3d 260, 270-72 (2d Cir. 2006) (stating that "preventing a terrorist from bombing the subways constitutes a special need that is distinct from ordinary post hoc criminal investigation"). As the FISA Court of Review has noted, "all the other courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information." In re Sealed Case, 310 F.3d 717, 742 (FISA Ct. Rev. 2002); see Gov't Mem. at 10 & n.7. ~~(S)~~

To require, as Yahoo suggests, a court order for each U.S. person whose communications are incidentally acquired would make little sense, impose an impossible burden on the Government, and may ultimately require the Government to discontinue its collection of information under the Protect America Act. The Government cannot know the identity of U.S. persons whose communications it incidentally acquires in the course of foreign intelligence surveillance. Because "the imposition of a warrant requirement [would] be disproportionate and perhaps even disabling burden on the Executive, a warrant should not be required." See United States v. Bin Laden, 126 F. Supp. 2d 264, 273 (S.D.N.Y. 2000); see also, e.g., United States v. Truong Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980). ~~(S)~~

B. The Acquisition of the Communications of U.S. Persons Authorized by the Directives Is Reasonable Under the Fourth Amendment. ~~(S)~~

Where the warrant requirement is inapplicable, a search will comply with the Fourth Amendment so long as it is reasonable. See United States v. Knights, 534 U.S. 112, 118 (2001). The acquisition at issue here easily satisfies this constitutional requirement, even though it will entail the collection of communications in which U.S. persons have a reasonable expectation of

privacy. Reasonableness under the Fourth Amendment must be evaluated under "the totality of the circumstances," considering "on the one hand, the degree to which [the search] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." See Knights, 534 U.S. at 118-19. Applying this test, the acquisition authorized by the directives must be upheld. ~~(S)~~

As the Supreme Court has recognized, "It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation." See Haig v. Agee, 453 U.S. 280, 307 (1981) (internal quotation marks omitted). With respect to U.S. persons whose communications are targeted or incidentally acquired, Congress and the Executive Branch have acted in concert to develop a framework with specific procedures and safeguards to ensure that acquisitions under the directives implicate the privacy of such U.S. persons only in a manner that is both targeted and minimal. See 50 U.S.C. § 1805B(a). When these extensive safeguards are considered in light of the overriding importance of the Government's interest, the acquisitions are manifestly reasonable under the Constitution. ~~(S)~~

First, before a directive may be issued, the Protect America Act requires the Government to adopt reasonable procedures for determining that the target of an acquisition under the Act is reasonably believed to be located outside the United States. See 50 U.S.C. § 1805B(a)(1). This Court recently reviewed and upheld certain targeting procedures the Government uses under the Protect America Act. See Mem. Op. and Order, [redacted] at 24 (Foreign Intel. Surv. Ct. Jan. 15, 2008) ("Procedures Op."). [6] The Protect America

[6] These targeting procedures, moreover, contain specific provisions designed to ensure that the privacy interests of U.S. persons are properly safeguarded. For example, the procedures require the prompt reporting of any incident of non-compliance to the Department of Justice and the Office of the Director of National Intelligence (including the ODNI Civil Liberties Protection Officer). See, e.g., [redacted] Further, the procedures state that [redacted]

Act also mandates that the Attorney General and Director of National Intelligence certify that a significant purpose of the acquisition is to acquire foreign intelligence information and that the acquisition involves obtaining such information with the assistance of a service provider. See id. §§ 1805B(a)(3)-(4). All of these requirements significantly constrain the scope of the collection under the directives and help ensure that the collection is carefully targeted to obtain foreign intelligence information in a reasonable manner. ~~(S)~~

Second, the Government must comply with section 2.5 of Executive Order 12333 before U.S. persons abroad may become targets of an acquisition. This provision requires the Attorney General to determine that "there is probable cause to believe that the [surveillance] technique is directed against a foreign power or an agent of a foreign power." See Executive Order 12333 § 2.5; [redacted] In approving foreign intelligence surveillance, courts have repeatedly looked to the Attorney General's determination under section 2.5 as an important factor in assessing the reasonableness of the surveillance. See In re Sealed Case, 310 F.3d at 746; Bin Laden, 126 F. Supp. 2d at 279 & n.18. ~~(S)~~

The incidental collection of communications of U.S. persons who are communicating with foreign intelligence targets abroad pursuant to the directives is also consistent with the Fourth Amendment. The lawful authority to conduct surveillance of one individual obviously includes the authority to collect that individual's communications with others. Accordingly, courts have routinely held that the incidental collection of third-party communications in the course of an otherwise lawful search does not render the search unreasonable.[7] This principle

[redacted] and will promptly report the incident to the Department of Justice and the Office of the Director of National Intelligence (including the ODNI Civil Liberties Protection Officer). Id. at 3, 6. ~~(S)~~

[7] See, e.g., United States v. Figueroa, 757 F.2d 466, 472-73 (2d Cir. 1985) ("the mere fact that Title III allows interception of conversations of 'others as yet unknown' does not render the statute unconstitutional");

applies equally in the foreign intelligence context. See United States v. Butenko, 494 F.2d 593, 608 (3d Cir. 1974) ("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."); United States v. Brown, 484 F.2d 418, 425 (5th Cir. 1973) (recording by "happenstance" of a U.S. person's communications pursuant to a lawful, warrantless wiretap authorized by the Attorney General for foreign intelligence purposes does not violate the Fourth Amendment); United States v. Clay, 430 F.2d 165, 170-72 (5th Cir. 1970), rev'd on other grounds, 403 U.S. 698 (1971) (same); Bin Laden, 126 F. Supp. 2d at 281 ("acknowledg[ing] that the combination of Verdugo-Urquidez and the incidental interception cases [cited above] would permit the surveillance if the Government had not been aware of [the U.S. person's] identity or of his complicity in the enterprise"). ~~(S)~~

For both categories of U.S. person communications, the minimization procedures the Government employs pursuant to the Protect America Act further supports the reasonableness of the acquisition. See 50 U.S.C. § 1805B(a)(5). These procedures must meet the statutory definition in FISA. Thus, they must be reasonably designed in light of the purpose and technique of the particular surveillance to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting U.S. persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information. See id.; 50 U.S.C. § 1801(h). These minimization procedures, which

---

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); Bin Laden, 126 F. Supp. 2d at 280 ("The Government properly asserts that in the Title III context, incidental interception of a person's conversations during an otherwise lawful surveillance is not violative of the Fourth Amendment."). (U)

contain [redacted] generally require, among other things, the deletion of U.S. person identities from intelligence reports based on foreign communications prior to dissemination except when the information constitutes foreign intelligence information, is necessary to understand foreign intelligence information, or is evidence of a crime. Courts have relied on such procedures in evaluating the reasonableness of surveillance. See In re Sealed Case, 310 F.3d at 740. Indeed, this Court, in its opinion upholding the targeting procedures used by the Government under the Protect America Act, emphasized 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." Procedures Op. at 13 n.15. In combination with the numerous other steps the Government must follow before it acquires the communications of U.S. persons (incidentally or otherwise), these minimization procedures ensure that the Government's acquisition of such persons' communications is reasonable under the Fourth Amendment. ~~(S)~~

The Government has used [redacted] minimization procedures to protect the privacy interests of U.S. persons in communications acquired in foreign intelligence surveillance programs for decades. As noted, foreign intelligence surveillance necessarily captures a significant amount of communications of U.S. persons, and the Executive Branch—with the knowledge and acquiescence of Congress—has relied on minimization procedures to help establish the constitutional reasonableness of the surveillance. This long-standing governmental practice further indicates that the minimization procedures the Government uses here ensure that the acquisition under the directives is reasonable. Cf. Camara v. Municipal Ct. of City and Cty. of San Francisco, 387 U.S. 523, 537 (1967) (explaining that among the "persuasive factors" supporting the reasonableness of administrative inspections is a "long history of judicial and

public acceptance"). 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 of communications for foreign intelligence purposes that does not fall within the ambit of FISA. ~~(S)~~

CONCLUSION (U)

For the reasons stated above and in its other filings submitted in this matter, the United States of America requests that this Court grant its motion for an order compelling Yahoo's compliance with the lawful directives of the Director of National Intelligence and Attorney General.[8] ~~(S)~~

[8] The Government recognizes that portions of the Protect America Act are scheduled to sunset in the near future. This fact does not affect this litigation, however, because Section 6(d) of the Protect America Act (which is not subject to the sunset contained in Section 6(c) of the Protect America Act) explicitly provides that "[a]uthorizations 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." Further, this Court's authority to enforce such directives under 50 U.S.C. § 1850B(g) is unaffected because Section 6(d) provides, relevant part, that "[s]uch acquisitions shall be governed by the applicable provisions of such amendments." (U)

Respectfully submitted,

Matthew G. Olsen
Deputy Assistant Attorney General

John A. Eisenberg
Deputy Assistant Attorney General

[redacted]
Counsel to the Assistant Attorney General

Office of Legal Counsel
U.S. Department of Justice

John C. Demers
Deputy Assistant Attorney General

[redacted]
Counsel to the Assistant Attorney General

[redacted]
Attorney Advisors
Office of Intelligence Policy and Review

[redacted]
Counsel for National Security Law & Policy
Office of Law and Policy

National Security Division
U.S. Department of Justice