~~TOP SECRET/TSSCI~~

United States Foreign Intelligence Surveillance Court of Review

---

No. 08-01 (S)

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

YAHOO! INC., (U)

Petitioner, Appellant.

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

[Hon. Reggie B. Walton, U.S. District Judge] (U)

Before

Selya, Chief Judge,
Winter and Arnold, Senior Circuit Judges. (U)

Marc J. Zwillinger, with whom Sonnenschein Nath & Rosenthal, LLP was on brief, for petitioner.

Gregory G. Garre, Acting Solicitor General, with whom 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, [redacted] Office of Legal Counsel, [redacted] Civil Division, and Matthew G. Olsen, John C. Demers, [redacted] National Security Division,

United States Department of Justice, were on brief, for respondent. (U)

August 22, 2008 (U)

SELYA, Chief Judge. This petition for review stems from directives issued to the petitioner, Yahoo! Inc., pursuant to a now-expired set of amendments to the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. §§ 1801-1871 (2007). Among other things, those amendments, known as the Protect America Act of 2007 (PAA), Pub. L. No. 110-55, 121 Stat. 552, authorized the United States to direct communications service providers to assist it in acquiring foreign intelligence when those acquisitions targeted third persons (such as the service provider's customers) reasonably believed to be located outside the United States. Having received [redacted] such directives, the petitioner challenged their legality before the Foreign Intelligence Surveillance Court (FISC). When that court found the directives lawful and compelled obedience to them, the petitioner brought this petition for review. (S)

As framed, the petition presents matters of both first impression and constitutional significance. At its most elemental level, the petition requires us to weigh the nation's security interests against the Fourth Amendment privacy interests of United States persons. (U)

After a careful calibration of this balance and consideration of the myriad of legal issues presented, we affirm

the lower court's determinations that the directives at issue are lawful and that compliance with them is obligatory. (S)

I. THE STATUTORY FRAMEWORK (U)

On August 5, 2007, Congress enacted the PAA, codified in pertinent part at 50 U.S.C. §§ 1805a to 1805c, as a measured expansion of FISA's scope. Subject to certain conditions, the PAA allowed the government to conduct warrantless foreign intelligence surveillance on targets (including United States persons) "reasonably believed" to be located outside the United States.[1] 50 U.S.C. § 1805b(a). This proviso is of critical importance here. (S)

Under the new statute, the Director of National Intelligence (DNI) and the Attorney General (AG) were permitted to authorize, for periods of up to one year, "the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States" if they determined that the acquisition met five specified criteria. Id. These criteria included (i) that reasonable procedures were in place to ensure that the targeted person was reasonably believed to be located outside the United States; (ii) that the acquisitions did not

[1]We refer to the PAA in the past tense because its provisions expired on February 16, 2008. (U)

constitute electronic surveillance;[2] (iii) that the surveillance would involve the assistance of a communications service provider; (iv) that a significant purpose of the surveillance was to obtain foreign intelligence information; and (v) that minimization procedures in place met the requirements of 50 U.S.C. § 1801(h). Id. § 1805b(a)(1)-(5). Except in limited circumstances (not relevant here), this multi-part determination was required to be made in the form of a written certification "supported as appropriate by affidavit of appropriate officials in the national security field." Id. § 1805b(a). Pursuant to this authorization, the DNI and the AG were allowed to issue directives to "person[s]" – a term that includes agents of communications service providers – delineating the assistance needed to acquire the information. Id. § 1805b(e); see id. § 1805b(a)(3). (U)

The PAA was a stopgap measure. By its terms, it sunset on February 16, 2008. Following a lengthy interregnum, the lapsed provisions were repealed on July 10, 2008, through the instrumentality of the FISA Amendments Act of 2008, Pub. L. No. 110-261, § 403, 122 Stat. 2436, 2473 (2008). But because the certifications and directives involved in the instant case were

---

[2]The PAA specifically stated, however, that "[n]othing in the definition of electronic surveillance . . . shall be construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States." 50 U.S.C. § 1805a. (U)

issued during the short shelf life of the PAA, they remained in effect. See FISA Amendments Act of 2008 § 404(a)(1). We therefore assess the validity of the actions at issue here through the prism of the PAA. (U)

[redacted] (S)

II. BACKGROUND (U)

Beginning in November of 2007, the government issued directives to the petitioner commanding it to assist in warrantless surveillance of certain customers' [redacted] These directives were issued pursuant to

[3]We use the term "surveillance" throughout to refer generally to acquisitions of foreign intelligence information, [redacted] (U)

certifications that purported to contain all the information required by the PAA.[4] (S)

The certifications require certain protections above and beyond those specified by the PAA. For example, they require the AG and the National Security Agency (NSA) to follow the procedures set out under Executive Order 12333 § 2.5, 46 Fed. Reg. 59,941, 59,951 (Dec. 4, 1981),[5] before any surveillance is undertaken. Moreover, affidavits supporting the certifications spell out additional safeguards to be employed in effecting the acquisitions. This last set of classified procedures has not been included in the information transmitted to the petitioner. In essence, as implemented, the certifications permit surveillances conducted to obtain foreign intelligence for national security purposes when those surveillances are directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States. (S)

The government's efforts did not impress the petitioner, which refused to comply with the directives. On November 21, 2007,

[4]The original certifications were amended, and we refer throughout to the amended certifications and the directives issued in pursuance thereof. (S)

[5]Executive Order 12333 was amended in 2003, 2004, and 2008 through Executive Orders 13284, 13355, and 13470, respectively. Those amendments did not materially alter the provision relevant here. (U)

the government moved to compel compliance. Following amplitudinous briefing, the FISC handed down a meticulous opinion validating the directives and granting the motion to compel. (S)

The FISC's decision was docketed on April 25, 2008. Six business days later, the petitioner filed a petition for review. The next day, it moved for a stay pending appeal. The FISC refused to grant the stay. On May 12, the petitioner began compliance under threat of civil contempt. Since that date, the government has identified approximately [redacted] to be surveilled. (S)

On May 16, 2008, the petitioner moved in this court for a stay pending appeal. We reserved decision on the motion and compliance continued. We then heard oral argument on the merits and took the case under advisement. We have jurisdiction to review the FISC's decision pursuant to 50 U.S.C. § 1805b(i) inasmuch as that decision is the functional equivalent of a ruling on a petition brought pursuant 50 U.S.C. § 1805b(h). See In re Sealed Case, 310 F.3d 717, 721 (Foreign Int. Surv. Ct. Rev. 2002). (S)

III. ANALYSIS (U)

We briefly address a preliminary matter: standing. We then turn to the constitutional issues that lie at the heart of the petitioner's asseverational array.

A. Standing. (U)

Federal appellate courts typically review standing determinations de novo, see, e.g., Muir v. Navy Fed. Credit Union, 529 F.3d. 1100, 1105 (D.C. Cir. 2008), and we apply that standard of review here. (U)

The FISC determined that the petitioner had standing to mount a challenge to the legality of the directives based on the Fourth Amendment rights of third-party customers. At first blush, this has a counter-intuitive ring: it is common ground that litigants ordinarily cannot bring suit to vindicate the rights of third parties. See, e.g., Hinck v. United States, 127 S.Ct. 2011, 2017 n.3 (2007); Warth v. Seldin, 422 U.S. 490, 499 (1975). But that prudential limitation may in particular cases be relaxed by congressional action. Warth, 422 U.S. at 501; see Bennett v. Spear, 520 U.S. 154, 162 (1997) (recognizing that Congress can "modif[y] or abrogat[e]" prudential standing requirements). Thus, if Congress, either expressly or by fair implication, cedes to a party a right to bring suit based on the legal rights or interests of others, that party has standing to sue; provided, however, that constitutional standing requirements are satisfied. See Warth, 422 U.S. at 500-01. Those constitutional requirements are familiar; the suitor must plausibly allege that it has suffered an injury, which was caused by the defendant, and the effects of which can be

redressed by the suit. See id. at 498-99; N.H. Right to Life PAC v. Gardner, 99 F.3d 8, 13 (1st Cir. 1996). (S)

Here, the petitioner easily exceeds the constitutional threshold for standing. It faces an injury in the nature of the burden that it must shoulder to facilitate the government's surveillances of its customers; that injury is obviously and indisputably caused by the government through the directives; and this court is capable of redressing the injury. (S)

That brings us to the question of whether Congress has provided that a party in the petitioner's position may bring suit to enforce the rights of others. That question demands an affirmative answer. (U)

The PAA expressly declares that a service provider that has received a directive "may challenge the legality of that directive," 50 U.S.C. § 1805b(h)(1)(A), and "may file a petition with the Court of Review" for relief from an adverse FISC decision, id. § 1805b(i). There are a variety of ways in which a directive could be unlawful, and the PAA does nothing to circumscribe the types of claims of illegality that can be brought. We think that the language is broad enough to permit a service provider to bring a constitutional challenge to the legality of a directive regardless of whether the provider or one of its customers suffers

the infringement that makes the directive unlawful. The short of it is that the PAA grants an aggrieved service provider a right of action and extends that right to encompass claims brought by it on the basis of customers' rights. (U)

For present purposes, that is game, set, and match. As said, the petitioner's response to the government's motion to compel is the functional equivalent of a petition under section 1805b(h)(1)(A). The petitioner's claim, as a challenge to the constitutionality of the directives, quite clearly constitutes a challenge to their legality. Thus, the petitioner's Fourth Amendment claim on behalf of its customers falls within the ambit of the statutory provision. It follows inexorably that the petitioner has standing to maintain this litigation. ~~(S)~~

B. The Fourth Amendment Challenge. (U)

We turn now to the petitioner's Fourth Amendment arguments. In the Fourth Amendment context, federal appellate courts review findings of fact for clear error and legal conclusions (including determinations about the ultimate constitutionality of government searches or seizures) de novo. See, e.g., United States v. Martins, 413 F.3d 139, 146 (1st Cir. 2005); United States v. Runyan, 290 F.3d 223, 234 (5th Cir. 2002).

We therefore review de novo the FISC's conclusion that the surveillances carried out pursuant to the directives are lawful. (S)

The petitioner's remonstrance has two main branches. First, it asserts that the government, in issuing the directives, had to abide by the requirements attendant to the Warrant Clause of the Fourth Amendment. Second, it argues that even if a foreign intelligence exception to the warrant requirements exists and excuses compliance with the Warrant Clause, the surveillances mandated by the directives are unreasonable and, therefore, violate the Fourth Amendment. The petitioner limits each of its claims to the harm that may be inflicted upon United States persons. (S)

1. The Nature of the Challenge. As a threshold matter, the petitioner asserts that its Fourth Amendment arguments add up to a facial challenge to the PAA. The government contests this characterization, asserting that the petitioner presents only an as-applied challenge. We agree with the government. (S)

A facial challenge asks a court to consider the constitutionality of a statute without factual development centered around a particular application. See, e.g., Wash. State Grange v. Wash. State Repub. Party, 128 S.Ct. 1184, 1190 (2008). Here, however, there is a particularized record and the statute – the PAA – has been applied to the petitioner in a specific setting. The

petitioner's plaints take account of this setting. So viewed, they go past the question of whether the PAA is valid on its face – a question that would be answered by deciding whether any application of the statute passed constitutional muster, see, e.g., id. – and ask instead whether this specific application offends the Constitution. As such, the petitioner's challenge falls outside the normal circumference of a facial challenge. (S)

This makes perfect sense. Where, as here, a statute has been implemented in a defined context, an inquiring court may only consider the statute's constitutionality in that context; the court may not speculate about the validity of the law as it might be applied in different ways or on different facts. See Nat'l Endow. for the Arts v. Finley, 524 U.S. 569, 584 (1998); see also Yazoo & Miss. Valley R.R. Co. v. Jackson Vinegar Co., 226 U.S. 217, 220 (1912) (explaining that how a court may apply a statute to other cases and how far parts of the statute may be sustained on other facts "are matters upon which [a reviewing court] need not speculate"). (U)

We therefore deem the petitioner's challenge an as-applied challenge and limit our analysis accordingly. This means that, to succeed, the petitioner must prove more than a theoretical risk that the PAA could on certain facts yield unconstitutional

applications. Instead, it must persuade us that the PAA is unconstitutional as implemented here. (S)

2. The Foreign Intelligence Exception. The recurrent theme permeating the petitioner's arguments is the notion that there is no foreign intelligence exception to the Fourth Amendment's Warrant Clause.[6] The FISC rejected this notion, positing that our decision in In re Sealed Case confirmed the existence of a foreign intelligence exception to the warrant requirement. (S)

While the Sealed Case court avoided an express holding that a foreign intelligence exception exists by assuming arguendo that whether or not the warrant requirements were met, the statute could survive on reasonableness grounds, see 310 F.3d at 741-42, we believe that the FISC's reading of that decision is plausible. (S)

The petitioner argues correctly that the Supreme Court has not explicitly recognized such an exception; indeed, the Court reserved that question in United States v. United States District

---

[6]The Fourth Amendment reads:

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

U.S. Const. amend. IV. (U)

Court (Keith), 407 U.S. 297, 308-09 (1972). But the Court has recognized a comparable exception, outside the foreign intelligence context, in so-called "special needs" cases. In those cases, the Court excused compliance with the Warrant Clause when the purpose behind the governmental action went beyond routine law enforcement and insisting upon a warrant would materially interfere with the accomplishment of that purpose. See, e.g., Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995) (upholding drug testing of high-school athletes and explaining that the exception to the warrant requirement applied "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement[s] impracticable" (quoting Griffin v. Wisconsin, 483 U.S. 868, 873 (1987))); Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 620 (1989) (upholding regulations instituting drug and alcohol testing of railroad workers for safety reasons); cf. Terry v. Ohio, 392 U.S. 1, 23-24 (1968) (upholding pat-frisk for weapons to protect officer safety during investigatory stop).

The question, then, is whether the reasoning of the special needs cases applies by analogy to justify a foreign intelligence exception to the warrant requirement for surveillance undertaken for national security purposes and directed at a foreign power or an agent of a foreign power reasonably believed to be

located outside the United States. Applying principles derived from the special needs cases, we conclude that this type of foreign intelligence surveillance possesses characteristics that qualify it for such an exception. (S)

For one thing, the purpose behind the surveillances ordered pursuant to the directives goes well beyond any garden-variety law enforcement objective. It involves the acquisition from overseas foreign agents of foreign intelligence to help protect national security. Moreover, this is the sort of situation in which the government's interest is particularly intense. (S)

The petitioner has a fallback position. Even if there is a narrow foreign intelligence exception, it asseverates, a definition of that exception should require the foreign intelligence purpose to be the primary purpose of the surveillance. For that proposition, it cites the Fourth Circuit's decision in United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980). That dog will not hunt. (S)

This court previously has upheld as reasonable under the Fourth Amendment the Patriot Act's substitution of "a significant purpose" for the talismanic phrase "primary purpose." In re Sealed Case, 310 F.3d at 742-45. As we explained there, the Fourth Circuit's "primary purpose" language – from which the pre-Patriot Act interpretation of "purpose" derived – drew an "unstable,

unrealistic, and confusing" line between foreign intelligence purposes and criminal investigation purposes. Id. at 743. A surveillance with a foreign intelligence purpose often will have some ancillary criminal-law purpose. See id. The prevention or apprehension of terrorism suspects, for instance, is inextricably intertwined with the national security concerns that are at the core of foreign intelligence collection. See id. In our view the more appropriate consideration is the programmatic purpose of the surveillances and whether – as in the special needs cases – that programmatic purpose involves some legitimate objective beyond ordinary crime control. Id. at 745-46. (U)

Under this analysis, the surveillances authorized by the directives easily pass muster. Their stated purpose centers on garnering foreign intelligence. There is no indication that the collections of information are primarily related to ordinary criminal-law enforcement purposes. Without something more than a purely speculative set of imaginings, we cannot infer that the purpose of the directives (and, thus, of the surveillances) is other than their stated purpose. See, e.g., United States v. Chem. Found., Inc., 272 U.S. 1, 14-15 (1926) ("The presumption of regularity supports the official acts of public officers, and, in the absence of clear evidence to the contrary, courts presume that they have properly discharged their official duties."). ~~(S)~~

We add, moreover, that there is a high degree of probability that requiring a warrant would hinder the government's ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake. See, e.g., Truong Dinh Hung, 629 F.2d at 915 (explaining that when the object of a surveillance is a foreign power or its collaborators, "the government has the greatest need for speed, stealth, and secrecy"). The government has presented evidence that foreign-agent terrorist suspects often [redacted] The evidence also suggests that some potential foreign intelligence information [redacted] Compulsory compliance with the warrant requirement would introduce an element of delay, thus frustrating the government's ability to collect information in a timely manner. In some cases, that delay might well allow the window in which [redacted] or information is available to slam shut before a warrant can be secured. (~~TS~~/SI)

For these reasons, we hold that a foreign intelligence exception to the Fourth Amendment's warrant requirement exists when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers

or agents of foreign powers reasonably believed to be located outside the United States. (S)

3. Reasonableness. This holding does not grant the government carte blanche: even though the foreign intelligence exception applies in a given case, governmental action intruding on individual privacy interests must comport with the Fourth Amendment's reasonableness requirement. See United States v. Place, 462 U.S. 696, 703 (1983). Thus, the question here reduces to whether the PAA, as applied through the directives, constitutes a sufficiently reasonable exercise of governmental power to satisfy the Fourth Amendment. (S)

We begin with bedrock. The Fourth Amendment protects the right "to be secure . . . against unreasonable searches and seizures." U.S. Const. amend. IV. To determine the reasonableness of a particular governmental action, an inquiring court must consider the totality of the circumstances. Samson v. California, 547 U.S. 843, 848 (2006); Tennessee v. Garner, 471 U.S. 1, 8-9 (1985). This mode of approach takes into account the nature of the government intrusion and how the intrusion is implemented. See Garner, 471 U.S. at 8; Place, 462 U.S. at 703. The more important the government's interest, the greater the intrusion that may be

constitutionally tolerated. See, e.g., Michigan v. Summers, 452 U.S. 692, 701-05 (1981). (U)

The totality of the circumstances model requires the court to balance the interests at stake. See Samson, 547 U.S. at 848; United States v. Knights, 534 U.S. 112, 118-19 (2001). If the protections that are in place for individual privacy interests are sufficient in light of the governmental interest at stake, the constitutional scales will tilt in favor of upholding the government's actions. If, however, those protections are insufficient to alleviate the risks of government error and abuse, the scales will tip toward a finding of unconstitutionality. (U)

Here, the relevant governmental interest – the interest in national security – is of the highest order of magnitude. See Haig v. Agee, 453 U.S. 280, 307 (1981); In re Sealed Case, 310 F.3d at 746. Consequently, we must determine whether the protections afforded to the privacy rights of targeted persons are reasonable in light of this important interest. (U)

At the outset, we dispose of two straw men – arguments based on a misreading of our prior decision in Sealed Case. First, the petitioner notes that we found relevant six factors contributing to the protection of individual privacy in the face of a governmental intrusion for national security purposes. See In re Sealed Case, 310 F.3d at 737-41 (contemplating prior judicial

review, presence or absence of probable cause, particularity, necessity, duration, and minimization). On that exiguous basis, it reasons that our decision there requires a more rigorous standard for gauging reasonableness. (S)

This is a mistaken judgment. In Sealed Case, we did not formulate a rigid six-factor test for reasonableness. That would be at odds with the totality of the circumstances test that must guide an analysis in the precincts patrolled by the Fourth Amendment. We merely indicated that the six enumerated factors were relevant under the circumstances of that case. (S)

Second, the petitioner asserts that our Sealed Case decision stands for the proposition that, in order to gain constitutional approval, the PAA procedures must contain protections equivalent to the three principal warrant requirements: prior judicial review, probable cause, and particularity. That is incorrect. What we said there – and reiterate today – is that the more a set of procedures resembles those associated with the traditional warrant requirements, the more easily it can be determined that those procedures are within constitutional bounds. See id. at 737, 742. We therefore decline the petitioner's invitation to reincorporate into the foreign intelligence exception the same warrant requirements that we already have held inapplicable. (S)

Having placed Sealed Case into perspective, we turn to the petitioner's contention that the totality of the circumstances demands a finding of unreasonableness here. That contention boils down to the idea that the protections afforded under the PAA are insufficiently analogous to the protections deemed adequate in Sealed Case because the PAA lacks (i) a particularity requirement, (ii) a prior judicial review requirement for determining probable cause that a target is a foreign power or an agent of a foreign power, and (iii) any plausible proxies for the omitted protections. For good measure, the petitioner suggests that the PAA's lack of either a necessity requirement or a reasonable durational limit diminishes the overall reasonableness of surveillances conducted pursuant thereto.

The government rejoins that the PAA, as applied here, constitutes reasonable governmental action. It emphasizes both the protections spelled out in the PAA itself and those mandated under the certifications and directives. This matrix of safeguards comprises at least five components: targeting procedures, minimization procedures, a procedure to ensure that a significant purpose of a surveillance is to obtain foreign intelligence information, procedures incorporated through Executive Order 12333 § 2.5, and what we shall call "linking procedures" (procedures that

link [redacted] targets as outlined in an affidavit supporting the certifications). (TS/SI)

The record supports the government. Notwithstanding the parade of horribles trotted out by the petitioner, it has presented no evidence of any actual harm, any egregious risk of error, or any broad potential for abuse in the circumstances of the instant case. Thus, assessing the intrusions at issue in light of the governmental interest at stake and the panoply of protections that are in place, we discern no principled basis for invalidating the PAA as applied here. In the pages that follow, we explain our reasoning. (S)

The petitioner's arguments about particularity and prior judicial review are defeated by the way in which the statute has been applied. When combined with the PAA's other protections, the linking procedures and the procedures incorporated through the Executive Order are constitutionally sufficient compensation for any encroachments. (S)

The linking procedures – procedures that show that the [redacted] designated for surveillance are linked to persons reasonably believed to be overseas and otherwise appropriate targets – involve the application of "foreign intelligence factors." These factors are delineated in an ex parte appendix filed by the government. They also are described, albeit

with greater generality, in the government's brief. As attested by affidavits of the Director of the National Security Agency (NSA), the government identifies [redacted] surveillance for national security purposes based on information indicating that, for instance,

[redacted] Although the PAA itself does not mandate a showing of particularity, see 50 U.S.C. § 1805b(b), this pre-surveillance procedure strikes us as analogous to and in conformity with the particularity showing contemplated by Sealed Case. 310 F.3d at 740. ~~(TS/SI)~~

The presence of a linking procedure here would seem to alleviate a concomitant concern voiced by the petitioner: that its offices (and, thus, the places of surveillance) are located on United States soil. After all, the petitioner conceded at oral argument that this concern was rooted in concerns about particularity – and as we have said, those concerns have been palliated. ~~(S)~~

The procedures incorporated through section 2.5 of Executive Order 12333, made applicable to the surveillances through the certifications and directives, serve to allay the probable cause concern. That section states in relevant part:

> The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power.

46 Fed. Reg. at 59,951 (emphasis supplied). Thus, in order for the government to act upon the certifications, the AG first had to make a determination that probable cause existed to believe that the targeted person is a foreign power or an agent of a foreign power. Moreover, this determination was not made in a vacuum. The AG's decision was informed by the contents of an application made pursuant to Department of Defense (DOD) regulations. See DOD, Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons, DOD 5240.1-R, Proc. 5, Pt. 2.C (Dec. 1982). Those regulations required that the application include a statement of facts demonstrating both probable cause and necessity. See id. They also required a statement of the period

– not to exceed 90 days – during which the surveillance was thought to be required.[7] See id. (S)

That the definition of an "agent of a foreign power" is more expansive under the Executive Order than under the counterpart FISA provision dealing with United States persons, 50 U.S.C. § 1801(b)(2), gives us pause. The definition operable under the Executive Order includes among other persons a United States person who is an employee of a foreign power.[8] This is potentially troublesome because, taken literally, it could include, say, a clerical employee or manual laborer with no connection to matters touching upon national security. In an effort to parry this thrust, the government argues that the term, as applied under Executive Order 12333 over the course of more than two decades, eliminates the possibility that it will be extended to include innocuous employees. (S)

---

[7]At oral argument, the government augmented this description, stating that, under the DOD procedure, the NSA typically provides the AG with a two-to-three-page submission articulating the facts underlying the determination that the person in question is an agent of a foreign power; that the National Security Division of the Department of Justice writes its own memorandum to the AG; and that an oral briefing of the AG ensues. (S)

[8]At least one provision of the FISA Amendments Act of 2008, which took effect after the directives in this case were issued, also incorporates United States persons who are employees of foreign powers. See FISA Amendments Act of 2008 § 703(b)(1)(C)(ii) (codified at 50 U.S.C. § 1881b(b)(1)(C)(ii)). (U)

We need not cross this bridge today. Courts do not deal in hypotheticals, and evidence of a practice of defining the term "employee" to include innocuous persons is wholly lacking in the record before us. Here, moreover, the government has tendered a declaration of the DNI made under the penalty of perjury that discusses the particular targets affected by the directives in this case. That declaration (which deals in examples) contradicts any use of an overly expansive definition of "employee." Whether the use of a definition that includes innocuous employees would be impermissibly broad is, therefore, not before us. See, e.g., United States v. Duggan, 743 F.2d 59, 71 (2d Cir. 1984) (holding argument that FISA definition of "agent of a foreign power" was overly broad irrelevant in a case in which a different, clearly permissible definition had been applied). (S)

The petitioner's additional criticisms about the surveillances can be grouped into concerns about potential abuse of executive discretion and concerns about the risk of government error (including inadvertent or incidental collection of information from non-targeted United States persons). We address these groups of criticisms sequentially. (S)

The petitioner suggests that, by placing discretion entirely in the hands of the Executive Branch without prior

judicial involvement, the procedures cede to that Branch overly broad power that invites abuse. But this is little more than a lament about the risk that government officials will not operate in good faith. That sort of risk exists even when a warrant is required. In the absence of a showing of fraud or other misconduct by the affiant, the prosecutor, or the judge, a presumption of regularity traditionally attaches to the obtaining of a warrant. See, e.g., McSurely v. McClellan, 697 F.2d 309, 323-24 (D.C. Cir. 1982). (S)

Here – where an exception affords relief from the warrant requirement – common sense suggests that we import the same presumption. Once we have determined that protections sufficient to meet the Fourth Amendment's reasonableness requirement are in place, there is no justification for assuming, in the absence of evidence to that effect, that those prophylactic procedures have been implemented in bad faith. (S)

Similarly, the fact that there is some potential for error is not a sufficient reason to invalidate the surveillances. The petitioner complains that approximately [redacted] of the [redacted] accounts that the government initially identified for surveillance have proved to be closed or nonexistent. It asserts that this indicates that errors plague the identification process and that

the systems for error-prevention are deficient. Building on this foundation, it suggests that because most of its account holders are United States persons, the risk of identification error creates an intolerable risk of surveilling non-targeted United States persons. (S)

This argument is woven exclusively out of gossamer strands of speculation and surmise. The inclusion of nonexistent accounts could not have caused any harm, and there is no solid evidence that any of the closed accounts were misidentified. They may very well have belonged to targeted persons and been closed between the time of the original identification and the time that surveillance started. (S)

Equally as important, some risk of error exists under the original FISA procedures – procedures that received our imprimatur in Sealed Case, 310 F.3d at 746. A prior judicial review process does not ensure that the types of errors complained of here (say, a misidentification arising out of the misspelling of an account holder's name) would have been prevented. (S)

It is also significant that effective minimization procedures are in place. These procedures serve as an additional backstop against identification errors as well as a means of reducing the impact of incidental intrusions into the privacy of

non-targeted United States persons. The minimization procedures implemented here are almost identical to those used under FISA to ensure the curtailment of both mistaken and incidental acquisitions. These minimization procedures were upheld by the FISC in this case, and the petitioner stated at oral argument that it is not quarreling about minimization but, rather, about particularity. Thus, we see no reason to question the adequacy of the minimization protocol. (S)

The petitioner's concern with incidental collections is overblown. It is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful.[9] See, e.g., United States v. Kahn, 415 U.S. 143, 157-58 (1974); United States v. Schwartz, 535 F.2d 160, 164 (2d Cir. 1976). The government assures us that it does not maintain a database of incidentally collected information from non-targeted United States persons, and there is no evidence to the contrary. On these facts, incidentally collected communications of non-targeted United States persons do not violate the Fourth Amendment. (S)

---

[9]The petitioner has not charged that the Executive Branch is surveilling overseas persons in order intentionally to surveil persons in the United States. Because the issue is not before us, we do not pass on the legitimacy vel non of such a practice. (S)

To the extent that the petitioner may be concerned about the adequacy of the targeting procedures, it is worth noting that those procedures include provisions designed to prevent errors. The government undertakes monitoring to ensure that the targeted person has not entered the United States. If he or she has, the procedures require immediate cessation of surveillance, with limited exceptions, the destruction of communications acquired since the person entered the United States, and a report of the incident to various officials within 72 hours. Furthermore, a PAA provision codified at 50 U.S.C. § 1805b(d) requires the AG and the DNI to assess compliance with those procedures and to report to Congress semi-annually. ~~(S)~~

4. A Parting Shot. The petitioner fires a parting shot. It presented for the first time at oral argument a specific example of an invasion of privacy in which the government could acquire [redacted] The petitioner argues that in this way the PAA and the implementing directives make [redacted] It says that the issue is properly before us because the directives allow the government to ask for

such [redacted] at any time, and if such a request is forthcoming the petitioner will be obligated to honor it. (S)

This parting shot may have been waived by the failure to urge it either before the FISC or in the petitioner's pre-argument filings in this court. We need not probe that point, however, because the petitioner is firing blanks: no communications falling within this description have been sought to date. Were the government to request [redacted] there are safeguards in place that may meet the reasonableness standard. These include the minimization procedures discussed above as well as a [redacted] This review is designed to ensure that the government does not surveil [redacted] (TS//SI)

[redacted]

heretofore been targeted, the petitioner has not yet experienced the type of harm about which it complains. Thus, even though the directives allow for such an acquisition, that bare possibility does not factor into our consideration of the constitutionality of the directives as applied here. See Duggan, 743 F.2d at 71. (S)

We do, however, direct the government promptly to notify the petitioner if it obtains from the petitioner [redacted] That should be fully sufficient to preserve the petitioner's ability to challenge any such acquisition, should one occur in the future. (S)

5. Recapitulation. After assessing the prophylactic procedures applicable here, including the provisions of the PAA, the affidavits supporting the certifications, section 2.5 of Executive Order 12333, and the declaration mentioned above, we conclude that they are very much in tune with the considerations discussed in Sealed Case. Collectively, these procedures require a showing of particularity, a meaningful probable cause determination, and a showing of necessity. They also require a durational limit not to exceed 90 days – an interval that we

previously found reasonable.[11] See In re Sealed Case, 310 F.3d at 740. Finally, the risks of error and abuse are within acceptable limits and effective minimization procedures are in place. (U)

Balancing these findings against the vital nature of the government's national security interest and the manner of the intrusion, we hold that the surveillances at issue satisfy the Fourth Amendment's reasonableness requirement. (U)

IV. CONCLUSION (U)

Our government is tasked with protecting an interest of utmost significance to the nation – the safety and security of its people. But the Constitution is the cornerstone of our freedoms, and government cannot unilaterally sacrifice constitutional rights on the alter of national security. Thus, in carrying out its national security mission, the government must simultaneously fulfill its constitutional responsibility to provide reasonable protections for the privacy of United States persons. The judiciary's duty is to hold that delicate balance steady and true.

---

[11]This time period was deemed acceptable because of the use of continuing minimization procedures. In re Sealed Case, 310 F.3d at 740. Those minimization procedures are nearly identical to the minimization procedures employed in this case. See text supra. (S)

We believe that our decision to uphold the PAA as applied in this case comports with that solemn obligation. In that regard, we caution that our decision does not constitute an endorsement of broad-based, indiscriminate executive power. Rather, our decision recognizes that where the government has instituted several layers of serviceable safeguards to protect individuals against unwarranted harms and to minimize incidental intrusions, its efforts to protect national security should not be frustrated by the courts. This is such a case. (U)

We need go no further. The decision granting the government's motion to compel is affirmed; the petition for review is denied and dismissed; and the motion for a stay is denied as moot. (U)

So Ordered. (U)

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

Declassify on: August 22, 2033