

United States Foreign Intelligence Surveillance Court
of Review.

In re DIRECTIVES [redacted text]^{FN*} PURSUANT
TO SECTION 105B OF the FOREIGN INTELLI-
GENCE SURVEILLANCE ACT.

FN* The text and footnotes that have been
redacted from this opinion contain classified
information.

[redacted text], Petitioner, Appellant.

No. 08-01.

Aug. 22, 2008.

Background: Communications service provider peti-
tioned for review of a decision of the Foreign Intelli-
gence Surveillance Court, Reggie B. Walton, District
Judge, finding directives issued to the service pro-
vider by the United States pursuant to the Protect
America Act (PAA), commanding the service pro-
vider to assist in warrantless surveillance of certain
customers reasonably believed to be outside the
United States, lawful, and compelling obedience to
the directives.

Holdings: The Foreign Intelligence Surveillance
Court of Review, Selya, Chief Judge, held that:

- (1) service provider had standing to challenge the
directives;
- (2) service provider's challenge was an as-applied
challenge to the PAA; and
- (3) PAA, as applied through the directives, satisfied
the Fourth Amendment's reasonableness requirement.

Petition denied.

*1006 [redacted text].

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. Eisen-
berg, Office of the Deputy Attorney General, John R.
Phillips, Office of Legal Counsel, Sharon Swingle,
Civil Division, and Matthew G. Olsen, John C.
Demers, Jamil N. Jaffer, Andrew H. Tannenbaum,
and Matthew A. Anzaldi, National Security Division,
United States Department of Justice, were on brief,
for respondent.

Before SELYA, Chief Judge, WINTER and
ARNOLD, Senior Circuit Judges.

SELYA, Chief Judge.

This petition for review stems from directives issued
to the petitioner [redacted text] 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 pro-
viders to assist it in acquiring foreign intelligence
when those acquisitions targeted third persons (such
as the service provider's customers) reasonably be-
lieved to be located outside the United States. Having
received [redacted text] such directives, the petitioner
challenged their legality before the Foreign Intelli-
gence Surveillance Court (FISC). When that court
found the directives lawful and compelled obedience
to them, the petitioner brought this petition for re-
view.

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.

After a careful calibration of this balance and consid-
eration of the myriad of legal issues presented, we
affirm the lower court's determinations that the direc-
tives at issue are lawful and that compliance with
them is obligatory.

I. THE STATUTORY FRAMEWORK

On August 5, 2007, Congress enacted the PAA, codi-
fied 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 surveil-
lance on targets (including United States persons)
“reasonably believed” to be located outside the
United States.^{FN1} 50 U.S.C. § 1805b(a). This proviso
is of critical importance here.

FN1. We refer to the PAA in the past tense
because its provisions expired on February
16, 2008.

*1007 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 informa-

tion 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 constitute electronic surveillance;^{FN2} (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).

FN2. 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.

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 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.

[redacted text]

II. BACKGROUND

Beginning in [redacted text] 2007, the government issued directives to the petitioner commanding it to assist in warrantless surveillance of certain customers [redacted text and footnote ^{FN3}]. These directives were issued pursuant to certifications that purported to contain all the information required by the

PAA.^{FN4}

FN3. [redacted text]

FN4. The original certifications were amended, and we refer throughout to the amended certifications and the directives issued in pursuance thereof.

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),^{FN5} 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 *1008 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.

FN5. 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.

The government's efforts did not impress the petitioner, which refused to comply with the directives. On [redacted text], 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.

The FISC's decision was docketed on [redacted text]. 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 [redacted text], the petitioner began compliance under threat of civil contempt. [redacted text]

On [redacted text], 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).

III. ANALYSIS

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.

[1] 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.

[2][3][4] 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*, 550 U.S. 501, 127 S.Ct. 2011, 2017 n. 3, 167 L.Ed.2d 888 (2007); *Warth v. Seldin*, 422 U.S. 490, 499, 95 S.Ct. 2197, 45 L.Ed.2d 343 (1975). But that prudential limitation may in particular cases be relaxed by congressional action. *Warth*, 422 U.S. at 501, 95 S.Ct. 2197; *see Bennett v. Spear*, 520 U.S. 154, 162, 117 S.Ct. 1154, 137 L.Ed.2d 281 (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, 95 S.Ct. 2197. 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, 95 S.Ct. 2197; *N.H. Right to Life PAC v. Gardner*, 99 F.3d 8, 13 (1st Cir.1996).

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.

*1009 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.

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.

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.

B. The Fourth Amendment Challenge.

[5] 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.

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 ex-

cuses 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.

[6] **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.

[7] 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*, --- U.S. ---, 128 S.Ct. 1184, 1190, 170 L.Ed.2d 151 (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 complaints 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 *1010 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.

[8] 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, 118 S.Ct. 2168, 141 L.Ed.2d 500 (1998); *see also Yazoo & Miss. Valley R.R. Co. v. Jackson Vinegar Co.*, 226 U.S. 217, 220, 33 S.Ct. 40, 57 L.Ed. 193 (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").

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.

2. *The Foreign Intelligence Exception.* The recur-

rent theme permeating the petitioner's arguments is the notion that there is no foreign intelligence exception to the Fourth Amendment's Warrant Clause.^{FN6} 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.

FN6. 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.

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.

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 Court (Keith)*, 407 U.S. 297, 308-09, 92 S.Ct. 2125, 32 L.Ed.2d 752 (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, 115 S.Ct. 2386, 132 L.Ed.2d 564 (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, 107 S.Ct. 3164, 97 L.Ed.2d 709 (1987))); *Skinner v. Ry. Labor Execs. Ass'n*, 489 U.S. 602, 620, 109 S.Ct. 1402, 103 L.Ed.2d 639 (1989) (upholding regulations instituting drug and alcohol testing of railroad workers for

safety reasons),*1011 *cf. Terry v. Ohio*, 392 U.S. 1, 23-24, 88 S.Ct. 1868, 20 L.Ed.2d 889 (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.

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.

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.

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.

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, 47 S.Ct. 1, 71 L.Ed. 131 (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.").

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"). [redacted text] Compulsory compliance *1012 with the warrant requirement would introduce an element of delay, thus frustrating the government's ability to collect information in a timely manner. [redacted text]

[9] 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.

[10] **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, 103 S.Ct. 2637, 77 L.Ed.2d 110 (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.

[11][12] 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, 126 S.Ct. 2193, 165 L.Ed.2d 250 (2006); *Tennessee v. Garner*, 471 U.S. 1, 8-9, 105 S.Ct. 1694, 85 L.Ed.2d 1 (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, 105 S.Ct. 1694; *Place*, 462 U.S. at 703, 103 S.Ct. 2637. 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, 101 S.Ct. 2587, 69 L.Ed.2d 340 (1981).

The totality of the circumstances model requires the court to balance the interests at stake. *See Samson*, 547 U.S. at 848, 126 S.Ct. 2193; *United States v. Knights*, 534 U.S. 112, 118-19, 122 S.Ct. 587, 151 L.Ed.2d 497 (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.

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, 101 S.Ct. 2766, 69 L.Ed.2d 640 (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.

At the outset, we dispose of two straw 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.

This is a mistaken judgment. In *Sealed Case*, we did not formulate a rigid six-factor test for reasonableness. That would *1013 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.

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.

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 [redacted text] procedures [redacted text] outlined in an affidavit supporting the certifications.

The record supports the government. Notwithstanding the parade of horrors 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.

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 [redacted text] procedures and the procedures incorporated through the Executive Order are constitutionally sufficient compensation for any encroachments.

The [redacted text] procedures [redacted text] are delineated in an ex parte appendix filed by the government. They also are described, albeit with greater generality, in the government's brief. [redacted text] 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*1014 contemplated by *Sealed Case*. 310 F.3d at 740.

[redacted text]

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.^{FN7} *See id.*

FN7. 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.

[redacted text and footnote^{FN8}]

FN8. [redacted text]

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.

[13] 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).

[14] 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*1015 procedures have been implemented in bad faith.

Similarly, the fact that there is some potential for

error is not a sufficient reason to invalidate the surveillances. [redacted text]

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 [redacted text] would have been prevented.

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.

[15] 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.^{FN9} See, e.g., *United States v. Kahn*, 415 U.S. 143, 157-58, 94 S.Ct. 977, 39 L.Ed.2d 225 (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.

FN9. 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.

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. [redacted text] 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.

4. A Parting Shot. The petitioner fires a parting shot. It presented for the first time at oral argument a specific privacy concern that could possibly arise under the directives. 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 issue falling within this description has arisen to date. Were such an issue to arise, there are safeguards in place that may meet the reasonableness standard. We do, however, direct the government promptly to notify the petitioner if this issue arises under the directives.^{FN10}

FN10. [redacted text]

The foregoing paragraph is a summary of our holding on this issue. We discuss with greater specificity the petitioner's argument, the government's safeguards, and our order in the classified version of this opinion.

***1016 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.^{FN11} 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.

FN11. 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*.

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.

IV. CONCLUSION

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 altar 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.

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.

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.

So Ordered.

ORDER

WHEREAS,

1. An opinion that addresses and resolves issues of statutory and constitutional significance has been filed under seal;
2. It would serve the public interest and the orderly administration of justice to publish this opinion;
3. Publication of an unredacted opinion would disclose materials that have been properly classified by the Executive Branch;
4. Redactions, after consultation with the Executive Branch, can be made to exclude such classified materials without distorting the content of the discussion of the statutory and constitutional issues;
5. Such redactions have been made by the Court;

IT IS HEREBY ORDERED that:

1. The redacted opinion shall be published in the usual manner employed by the United States Courts of Appeals.

*1017 2. Notwithstanding the publication of the redacted opinion, the parties and their counsel, and any agent of, or other person(s) working in concert with, any party or counsel, shall continue to handle and safeguard all classified information pertaining to this case in accordance with applicable security requirements and regulations and applicable orders issued by this Court or the FISC. No party or counsel (nor any agent of, or other person(s) working in concert with, any party or counsel) shall disclose publicly or to any unauthorized person or persons any classified information pertaining to this case.

3. Classified information pertaining to this case includes, but is not limited to, information that has been redacted from the classified version of the Court's opinion, such as the identity of the petitioner and the intelligence sources and methods at issue. That term also includes information derived from the case that would tend to reveal classified matters, such as the identity of the petitioner or the intelligence sources and methods at issue.

4. All court records in this case (including the proceedings before this Court and the FISC) that contain classified information shall be maintained under seal and in accordance with applicable security requirements and previous court orders. Such records shall not be disclosed publicly or to any unauthorized person or persons without the express permission of this Court first had and obtained (or in the case of lower court records, without the express permission of the FISC first had and obtained). No other documents containing classified information pertaining to this case, such as declarations, correspondence, memoranda, notes, drafts, or other communications, shall be disclosed publicly or to any unauthorized person or persons without the express permission of the Court first had and obtained. This Court shall act on any request to disclose court records or other documents containing classified information anent this case only after consultation with the Executive Branch.

5. As used herein, the term “classified information” includes any information, document, or portion of a document, not included in the published, redacted opinion, that has been and remains classified by an Executive Branch agency or official pursuant to applicable Executive Orders as “CONFIDENTIAL,”

“SECRET,” “TOP SECRET,” or additionally controlled as “SENSITIVE COMPARTMENTALIZED INFORMATION,” or any information, document, or portion of a document that has been derived from such classified information, whether in written, oral, or other form. The term “unauthorized person” refers to any individual or entity that has not been granted access by the Court to classified information pertaining to the case, or that has not, in accordance with applicable Executive Orders, (1) received the requisite security clearance, (2) signed an appropriate nondisclosure agreement, and (3) been determined to have a need to know the classified information at issue.

6. Publication of the redacted opinion shall not occur until 72 hours after the filing of this Order to allow the Executive Branch to notify affected persons of this Order and to make appropriate notifications to Congress.

7. Any violation of this Order shall immediately be brought to the Court's attention. The unauthorized use or disclosure of classified information pertaining to this case may violate federal criminal law and could result in civil or criminal penalties for contempt of court.

8. This Order supersedes the Order issued by the Court on January 5, 2009.

***1018** IT IS SO ORDERED, this 12th day of January, 2009, at 12:00 p.m. EST.

For.Intel.Surv.Rev.,2008.
In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act
551 F.3d 1004