~~TOP SECRET//SI//ORCON/NOFORN/FISA~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

[redacted] Docket Number: [redacted]

OPINION AND ORDER PROVIDING STATEMENT OF REASONS FOR DENIAL OF APPLICATION

This matter came before the Foreign Intelligence Surveillance Court (FISC) on the government's Verified Application (Application) in the above-captioned docket. As explained below, the Application is denied for failure to establish probable cause to believe that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a)(2)(B). This Opinion and Order provides the written statement of each reason for denial required by 50 U.S.C. § 1803(a)(1).

Procedural Background

The Application, which was submitted on October 3, 2024, seeks authorization under Title I of the Foreign Intelligence Surveillance Act (FISA), codified at 50 U.S.C. §§ 1801-1811, for the Federal Bureau of Investigation (FBI) to conduct [redacted] On the

[1] [redacted]

same date, the government also submitted in Docket Number [redacted] a Verified Submission of Standard Technique Description [redacted] describes how the FBI [redacted] and addresses certain issues presented by such surveillance. The Application incorporates the Technique Description by reference. Application at 18.

Finding the Application to present novel or significant issues of law, the Court appointed David S. Kris to serve as amicus curiae (Amicus) pursuant to § 1803(i)(2)(A). The Amicus and the government were directed to file briefs addressing the following issues:

> (a) Whether the Court should regard the Application as an application for electronic surveillance, such that the Court should entertain it under Title I of FISA; and
> (b) Whether the electronic surveillance for which the Application seeks approval is directed at any facility or place [redacted] used by [redacted] for purposes of the probable cause finding required by 1805(a)(2)(B).

Order Appointing Amicus Curiae (Oct. 17, 2024) at 6. The Amicus requested permission to address an additional issue: whether the "if known" qualifier in FISA's provision that an order approving electronic surveillance must specify "the nature and location of each of the facilities or places at which the electronic surveillance will be directed, *if known*" (50 U.S.C. § 1805(c)(1)(B) (emphasis added)) has been repealed by implication. The Court granted this request. The Amicus Brief and Government Response were timely filed on November 19, 2024, and December 9, 2024, respectively. The Court thanks the Amicus for his able assistance.

[redacted]

[redacted]

[2] From 2008 to 2015, the government sought and the FISC granted approval [redacted] as a form of pen register/trap-and-trace surveillance under Title IV of FISA (codified at 50 U.S.C. §§ 1841-1846). *Id.* at 3-4. [redacted] This case is the first since the issuance of this policy in which the government seeks FISC approval [redacted] *Id.*

[redacted]

This Case Involves an Application for Electronic Surveillance

The FISC has "jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth" in FISA. 50 U.S.C. § 1803(a)(1). FISA has a four-part definition of "electronic surveillance" which, as relevant here, encompasses

> (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents[3] of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be

[3] As used in Title I of FISA, the term "contents," "when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication." 50 U.S.C. § 1801(n).

> required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
> (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

50 U.S.C. § 1801(f).[4]

Section 1801(f)(3) and (f)(4)

The government and the Amicus agree that the Application seeks approval of electronic surveillance, albeit on different theories. The government posits that the Application seeks to conduct electronic surveillance under § 1801(f)(3), and the Amicus views the proposed surveillance as falling under § 1801(f)(4). Their disagreement hinges on whether, as the government contends [redacted] involves "acquisition . . . of the contents of any radio communication," thereby implicating subparagraph (f)(3). *See* Gov't Resp. at 6-7. On the Amicus's view, [redacted] involves acquiring radio transmissions [redacted] but those transmissions do not constitute "communications" for purposes of § 1801(f). *See* Amicus Br. at 11. Thus, for the Amicus, the applicable part of the "electronic surveillance" definition is at subparagraph (f)(4), which refers to acquiring information "other than from a wire or radio communication." *See id.* at 10-11. But the Amicus advises that, if the [redacted] were viewed as acquiring the contents of a radio communication, it should be regarded as electronic surveillance

[4] Subparagraph (f)(1) of this definition does not apply because the [redacted] does not involve "intentionally targeting" "a particular, known United States person who is in the United States." § 1801(f)(1). Subparagraph (f)(2) does not apply because the [redacted] does not involve acquiring "the contents of any wire communication," which FISA defines as "any communication *while it is being carried by a wire, cable, or other like connection* furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications." 50 U.S.C. § 1801(l) (emphasis added).

under subparagraph (f)(3). *See id.* at 11. Reciprocally, the government submits that, if (f)(3) is found inapplicable because contents of a radio communication are not acquired, the [redacted] should be regarded as electronic surveillance under (f)(4). *See* Gov't Resp. at 8.

Here, it is not necessary for the Court to decide whether [redacted] involves acquiring the contents of a radio communication because, as suggested by the government and the Amicus, the requested surveillance constitutes "electronic surveillance" either way: it falls under (f)(3) if it involves acquiring the contents of a radio communication and under (f)(4) if it does not. All that matters is that, as explained below, the [redacted] is "electronic surveillance."

That is so because [redacted] satisfies the other elements of both (f)(3) and (f)(4). Under (f)(3), the [redacted] constitutes an "intentional acquisition by an electronic, mechanical, or other surveillance device," [redacted] In addition, assuming per the government that a radio communication is subject to acquisition, "both the sender," i.e., the user of [redacted] "and all intended recipients," i.e., [redacted] "are located within the United States."[5] Turning to (f)(4) and assuming [redacted] does not involve acquiring information from a radio communication, [redacted] constitutes "use of an electronic, mechanical, or other surveillance device [redacted] in the United States for monitoring to acquire information."

[5] The government suggests that [redacted] is the *intended* recipient, even though [redacted] Gov't Resp. at 8. In any event, both candidates for the intended recipients [redacted] - are in the United States.

Finally, both (f)(3) and (f)(4) require "circumstances in which a person[6] has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." (For brevity, this Opinion will sometimes refer to such circumstances as "Fourth Amendment circumstances.") For reasons set out below, the Court finds that this requirement is also met.

Reasonable Expectation of Privacy and Warrant Requirement

The government concurs with the Amicus that, "'[i]n general, the courts in criminal cases have found a reasonable expectation of privacy and required probable cause and a warrant'" [redacted] Gov't Resp. at 6 n.5 (quoting Amicus Br. at 13).[7] They also agree that the [redacted] would involve Fourth Amendment circumstances; again, however, they get to that conclusion by different routes.

At a conceptual level, the Amicus argues that the Court should decide [redacted] is electronic surveillance as defined by FISA, and specifically that it involves Fourth Amendment circumstances, though such a decision could, if necessary, rest on "reasonable assumptions as to the expected facts – e.g., as to how long [redacted] how many non-targets will be surveilled, and whether or not it will acquire [redacted] private homes." Amicus Br. at 24.

---

[6] The Amicus asserts, and the government has not disputed, that this language refers to a hypothetical U.S. person, so that it does not matter for purposes of (f)(3) and (f)(4) whether the actual persons to be subject to the requested surveillance are protected by the Fourth Amendment. *See* Amicus Br. at 12. The FISC previously has taken the same approach, *see* [redacted] Docket No. [redacted] Mem. Op. at 8-9 (FISC [redacted]); [redacted] Docket No. [redacted], Order at 4-5 (FISC [redacted]), and does so again in this case.

[7] [redacted] at *9 [redacted] *report and recommendation adopted by* [redacted]

In the government's view, the Court need not be so definitive on the issue; rather, if an application presents "legal uncertainties" about the applicability of the Fourth Amendment, Gov't Resp. at 6, or "uncertainty . . . as to whether the facts of the case demonstrate there is a reasonable expectation of privacy," the Court should entertain it. Technique Description at 36. The government argues that, in close cases, its personnel should be able to apply for an electronic surveillance order, rather than having "to assume the risk of being wrong about whether a constitutionally protected expectation of privacy exists." *Id.* (internal quotation marks omitted).

The text of the statute provides guidance: because the FISC has "jurisdiction to hear applications for and grant orders approving electronic surveillance," § 1803(a)(1), the question is whether the application *seeks approval* of electronic surveillance. If an application properly describes the surveillance for which approval is sought, applying the definition of "electronic surveillance" to that description should be sufficient to determine whether the FISC has "jurisdiction to hear" the application under § 1803(a)(1).[8]

In this case, the Application requests authorization to conduc[redacted] whenever "there are reasonable grounds to believe [redacted] *Id.* at

[8] Some applications have omitted or inaccurately stated information possessed by the FBI that was material to whether the collection for which approval was sought was electronic surveillance or physical search as defined by the statute. (Title III of FISA, codified at 50 U.S.C. §§ 1821-1829, concerns physical searches, and "physical search" is defined at § 1821(5)). In response to such cases, the FISC issued a standing order in November 2021 to ensure that "each application . . . contains information necessary to evaluate whether the approvals requested are within the Court's authority under Titles I and III of FISA." *In re Electronic Surveillance and Physical Search Applications Submitted to the FISC*, Docket No. [redacted] Standing Order at 9 (FISC [redacted]).

21. "The FBI will effectuate [redacted] In one place the Application states that the duration of this requested approval is "until the FBI is able to identify [redacted] . . . or for a period of 120 days, whichever is sooner." Application at 19 (emphasis added). Other parts of the Application, however, make clear that the FBI seeks approval to [redacted][9]

Given these parameters, the Court finds that Fourth Amendment circumstances are presented [redacted] the requested authorization includes acquisition [redacted] are within their [redacted] This aspect of the [redacted] intrudes on the reasonable expectations of privacy of such users. The court in [redacted]

[9] [redacted]

[redacted] implicate individuals' reasonable expectations of privacy in information about constitutionally protected areas that otherwise could not be obtained without a search warrant.").[10]

[redacted] As a result, there is no basis for arguing that, under the third-party doctrine,[11] there is a reduced expectation of privacy in the data acquired. [redacted]

[10] *See also* [redacted] that placed defendant within his home constituted a Fourth Amendment search, requiring a warrant or application of an established exception to warrant requirement).

[11] As a general rule, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," so "the Government is typically free to obtain such

[redacted] involves Fourth Amendment circumstances because it intrudes into, and obtains information from within, residences and other sensitive areas by means not generally available to the public. Accordingly, the Court finds that the Application in this case is one "for . . . electronic surveillance" as that term is defined in § 1801(f), such that the Court has "jurisdiction to hear" it under § 1803(a)(1), without addressing the Amicus's arguments that Fourth Amendment circumstances are presented for other reasons. *See* Amicus Br. at 13-14 [redacted]

Probable Cause Findings Required by 50 U.S.C. § 1805(a)(2)

In order to grant an electronic surveillance application under Title I of FISA, the Court must make two probable cause findings "on the basis of the facts submitted by the applicant." 50 U.S.C. § 1805(a)(2). First, the Court must find probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power." § 1805(a)(2)(A). [redacted] as the target of the proposed electronic surveillance and pleads [redacted] as an agent of a foreign power as defined at 50 U.S.C. § 1801(b)(1)(A), i.e., a non-United States person who "acts in the United States as an officer or employee of a foreign power . . . irrespective of whether the person is inside the United States." [redacted]

---

information from the recipient without triggering Fourth Amendment protections." *Carpenter v. United States*, 585 U.S. 296, 308 (2018) (internal quotation marks omitted). In *Carpenter*, the Court declined to apply this principle to CSLI records in the possession of cell service providers, due to the privacy concerns presented by "a detailed chronicle of a person's physical presence compiled" from such records and the Court's conclusion that a cell phone user's exposure of location information to such a provider is not meaningfully voluntary. *Id.* at 313-15.

a foreign power as defined at 50 U.S.C. § 1801(a)(1). The probable-cause finding required by § 1805(a)(2)(A) is well-supported.

Second, the Court must find probable cause to believe that "*each* of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." § 1805(a)(2)(B) (emphasis added). For the reasons explained below, the facts submitted do not support this finding.

Interpretation of § 1805(a)(2)(B)

The Application proffers facts which the government submits are the only facilities at which this electronic surveillance is directed. *See* Application at 7-12. As described above, expected to acquire therefore presents the issue whether facilities such that § 1805(a)(2)(B) requires probable cause findings for them as well.

12

The Amicus contends that "the actual nature of the surveillance" determines the facilities at which the surveillance is directed, even if the government's objective is to ascertain [redacted] Amicus Br. at 29. Here, the surveillance involves acquiring [redacted] regardless of whether they belong to [redacted] In the government's view, electronic surveillance is directed at "that facility or place about which the government seeks information." *Id.* at 13; *see also id.* (suggesting that, for purposes of § 1805(a)(2)(B), ""is directed"" means "aimed at, focused on, or otherwise reflecting the objective of the electronic surveillance").

In arguing for this interpretation, the government notes that the target of an electronic surveillance is the individual or entity about whom or from whom information is sought. *See id.* at 12 (citing *In re Sealed* Case, 310 F.3d 717, 740 (FISCR 2002) (per curiam). But § 1805(a)(2)(B) does not use the term "target" or speak of "targeted facilities." Rather, the required probable cause

finding is that each facility or place at which surveillance is *directed* is being used or is about to be used by a foreign power or an agent of a foreign power. The definition of "target" provides little guidance on how to interpret the pertinent language.

The government also claims that "numerous prior decisions" of the FISC support its "position that 'is directed' at applies to that facility or place about which the Government seeks information." *Id.* at 13. The Court has a different understanding.

The government primarily relies on [redacted] Order and Mem. Op. [redacted] (discussed in Gov't Resp. at 14-17). In that case, the FISC rejected the government's argument that a proposed electronic surveillance by the National Security Agency (NSA) [redacted] For the most part, the proposed surveillance would acquire communications to or from particular [redacted] Contrary to the government's theory, the Court held that those [redacted] were the facilities at which this surveillance would be directed. The Court noted that the surveillance devices would use those [redacted] at 12. Applying the parts of the definition of "electronic surveillance" pertinent to that case, the Court found that "the electronic surveillance *is* the acquisition of the contents of communications." *Id.* at 8; *accord* [redacted] Docket No. [redacted] Op. at 10 (FISC [redacted]) (adopting same interpretation of § 1801(f)(2)) [redacted][13] Accordingly, *how*

[13] The parts of the "electronic surveillance" definition applicable in [redacted] were § 1801(f)(2) ("*the acquisition* by an electronic, mechanical, or other surveillance device *of the contents of any wire communication* to or from a person in the United States, without the consent

the acquisitions were directed determined *at what facilities the surveillance was directed* for purposes of § 1805(a)(2)(B). Thus, insofar as NSA planned to use "surveillance devices to select for acquisition" only communications to or from "the telephone numbers and e-mail addresses used as selectors," the Court found that such surveillance was directed at those [redacted] *In re* [redacted] at 8-9.[14]

[redacted] in this case will acquire [redacted] Under the interpretation of § 1805(a)(2)(B) adopted in [redacted] the proposed electronic surveillance is therefore directed at each of those [redacted]. This "interpretive approach *appropriately* focuses the Court's probable cause inquiry on the likelihood that the [facilities] . . . subject to acquisition are being used by" a targeted agent of a foreign power. [redacted] at 10 (emphasis added); *see also* [redacted] at 15 (rejecting interpretation under which "the judge's probable cause findings have no bearing on

---

of any party thereto, if such acquisition occurs in the United States") and § 1801(f)(4) ("the installation or use of an electronic, mechanical, or other surveillance device in the United States *for monitoring to acquire information*" under specified circumstances) (emphases added). As discussed above, the definition [redacted] in this case is at either § 1801(f)(4) or § 1801(f)(3) ("*the intentional acquisition* by an electronic, mechanical, or other surveillance device *of the contents of any radio communication*" under specified circumstances) (emphasis added). Under all of these definitions, the surveillance consists of the act of or the means of acquiring information.

[14] One form of surveillance at issue in [redacted] involved acquiring communications (sometimes called "abouts communications") that contained a reference to, but were not to or from, a selector email address. The Court found that this form of surveillance was also directed at particular [redacted] rather than at the [redacted] on which the surveillance [redacted] were placed. *Id.* at 10.

the salient question: whether the communications to be acquired will relate to the targeted foreign powers"). In contrast, under the government's interpretation of § 1805(a)(2)(B), it does not matter how likely it is that data will be acquired [redacted] used by persons who have no connection to [redacted]

The government points to statements in *In* [redacted] that NSA was interested only in communications related to particular [redacted] used by the targets. *See* Gov't Resp. at 15. It is apparent, however, that those statements were simply meant to explain why NSA [redacted][15] The government's subjective interest did not determine at what facilities the proposed surveillance was directed. [redacted] "NSA [redacted] to [redacted] *Id.* at 8. "These facts strongly suggest that the acquisition of the contents of communications - - - that is, the electronic surveillance itself - - - is directed at the [redacted] used as selectors." *Id.* at 9; *see also id.* ("because the surveillance" conducted under § 1801(f)(4) "consists of monitoring to acquire information, and the only information to be acquired relates to the [redacted] used as selectors, the electronic surveillance would be directed at those [redacted]

[15] For example, with regard to acquisition of abouts communications, the Court observed that [redacted] at 10 (emphasis added).

The government also attempts to harmonize the instant application with [redacted] by observing that, in the latter case, the [redacted] but ultimately only communications pertaining to selector [redacted] would be retained or used. *See* Gov't Resp. at 16, 19. So too, the government argues, [redacted] and the FBI will delete the non-targets' data after it completes that identification process. *See id.* at 16-17, 19. [redacted]

In this case the government concedes, as it must, that "[t]he manner [redacted] surveillance is conducted . . . will likely result in the *acquisition* of data from facilities other than [redacted] being used by the target." [redacted] (emphasis added). Limitations on how the FBI retains and uses data may help satisfy minimization requirements under 50 U.S.C. §§ 1801(h) and 1805(a)(3), but they cannot alter the fact that the FBI acquired the data in the first place.

Lack of Probable Cause Required by § 1805(a)(2)(B)

The proffer in this case does not establish probable cause to believe that each facility [redacted] – is being used or is about to be used by a foreign power or an agent of a foreign power and therefore does not support the finding required by § 1805(a)(2)(B). Against this conclusion, the government cites opinions in which the FISC authorized electronic surveillance or physical search, notwithstanding a possibility that facilities not used by, or property not owned, used or possessed by, a foreign power or an agent of a foreign power could be subject to surveillance or search.[16] *See* Technique Description at 38-40. Those cases are distinguishable simply because they involved facts that supported the required probable cause findings.

In [redacted] the FISC could not rule out the possibility that surveillance would be directed at a facility that was not used by a foreign power or an agent of a foreign power. [redacted] at 19. The Court noted, however, that "because the probable cause standard requires only a fair probability . . . its application frequently involves a non-trivial chance that it will turn out that what there was probable cause to believe in fact was not true." *Id.* at 23. Because there appeared [redacted] at 18-19, the Court found probable cause to believe that each facility at which the surveillance would be directed was being used or was about to be used by the targets.

[16] Under a provision analogous to § 1805(a)(2)(B), a FISC judge must find "probable cause to believe that . . . the premises or property to be searched is or is about to be owned, used, or possessed by, or is in transit to or from an agent of a foreign power or a foreign power" in order to grant a physical search application. 50 U.S.C. § 1824(a)(2)(B).

[redacted] physical search case, the FISC initially "was unable to find, on the basis of the government's original submissions, probable cause to believe that 'the premises or property proposed to be searched . . . is or is about to be owned, used, possessed by, or is in transit to or from an agent of a foreign power or a foreign power.'" [redacted] Docket Nos. [redacted] Op. and Supp. Ord. at 5 (FISC [redacted]) (quoting § 1824(a)(2)(B)). After the government revised the application to narrow the criteria for [redacted] the Court was able to make that probable cause finding, notwithstanding the residual possibility of [redacted] not owned, used or possessed by a target. *See id.*

It is highly probable, not just possible, [redacted] in this case would be directed at facilities that are not used by a foreign power or an agent of a foreign power. *See* Technique Description at 18 ("the FBI will likely obtain [redacted] not used by the target"); *id.* at 38 ([redacted] result in the acquisition of data from facilities other than the [redacted] being used by the target"). The Application describes [redacted] The likelihood [redacted] would acquire [redacted] that are not used by [redacted] is much too great for the probable cause finding required by § 1805(a)(2)(B) to be made. [redacted]

[redacted]

Because that is the crux of this case, the government is off the mark in relying on cases involving acquisition of non-target information from facilities or places used by targets, *in addition to* non-targets. Some types of shared-use facilities are encountered frequently.

> For example, it is common for family members or co-workers to share use of a telephone line [redacted]. Where one user of a shared facility is a valid FISA target, electronic surveillance of it may be authorized if there are adequate protections for how the government handles such non-target communications as may unavoidably be acquired.

[redacted] at 20. The shared-use cases cited by the government may be less prosaic, but they are not availing.

In *In re U.S. Person #1*,[17] Docket No. [redacted] Op. [redacted] at 12 (FISC [redacted]), the FISC authorized electronic surveillance targeting an agent of a foreign power at [redacted] The Court found probable cause to believe that the target was using or about to use [redacted] *Id.* at 2, 10. The Court authorized surveillance directed at [redacted] *Id.* at 12. "Given these technical constraints, it was appropriate to authorize the acquisition of [redacted] *Id.* By the same token, the circumstances of the case,

[17] Where the captions of cited cases include the names of individual targets, a generic identifier is substituted.

including the large volume of non-target information acquired [redacted] highlighted the need for post-acquisition minimization. *See id.* at 20-30 (finding minimization procedures insufficient regarding handling of certain non-target communications).

The physical search authorized in [redacted] Docket No. [redacted] Primary Ord. and Warrant at 3 (FISC [redacted] *In re* [redacted] involved similar circumstances. There was probable cause to believe [redacted] was used or about to be used by the targets. [redacted] hat were used by persons unrelated to the targets. *Id.*, Verified Application at 28. [redacted] *Id.* The Court authorized, among other things, such physical search, subject to special minimization procedures for handling information [redacted], Primary Ord. and Warrant at 7-10, upon finding probable cause to believe that "the premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from" the targets. *Id.* at 2. The Court's order described the authorized search as [redacted] *Id.* at 3. There is no opinion in that case, but the circumstances and scope of authorization are consistent with the reasoning of the Court in *In re U.S. Person #1*: The targets can be said to have used [redacted] even though they used [redacted] in a more precise and immediate sense. [redacted] prevented a search that would acquire only information pertaining to the targets' [redacted] the Court authorized search [redacted] subject to appropriate minimization of such data post-acquisition.

[redacted] case cited by the government is also inapposite. That surveillance [redacted] *In re U.S. Person #2*, Docket No. [redacted] Primary Ord. and Warrant at 8-9 (FISC [redacted]). Although there was no opinion explaining the disposition, the Court found probable cause to believe that the target was an agent of a foreign power and that "the facilities or places at which electronic surveillance will be directed are being used or about to be used by" the target, pursuant to § 1805(a)(2)(A)-(B). *Id.* at 2. The possibility of "inadvertently acquir[ing]" conversations of persons unrelated to the target stemmed from the fact that such persons may be [redacted] *Id.*, Verified Application at 81.

* * *

To be sure, some courts have found [redacted] to comport with the probable-cause requirements applicable in non-FISA law enforcement contexts. *See* Technique Description at 26-32 (discussing cases). But this case is subject to the specific requirements of FISA, which do not always align with those applicable to search or surveillance in domestic criminal investigations. *See In re Sealed Case*, 717 F.3d at 740 (because "FISA requires probable cause to believe the target is an agent of a foreign power . . . who uses or is about to use the targeted facility," it requires "more of a nexus between the target and the pertinent communications" than is required for a Title III wiretap in a domestic criminal investigation).

For the above-stated reasons, the Verified Application in Docket No. [redacted] is hereby DENIED because "the facts submitted by the applicant" do not support a finding of "probable cause to believe that . . . each of the facilities or places at which the electronic surveillance is being used, or is about to be used, by a foreign power or an agent of a foreign power," as required by 50

U.S.C. § 1805(a)(2)(B). Because denial is required for this reason, this Opinion does not reach other issues briefed. *See* Amicus Br. at 31-39; Gov't Resp. at 20-37.

ENTERED this 28th day of January, 2025.

ANTHONY J. TRENGA
Judge, United States Foreign
Intelligence Surveillance Court

I, [redacted] Deputy Clerk, FISC, certify that this document is a true and correct copy of the original.