

MAR 05 2020

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

LeeAnn Flynn Hall, Clerk of Court

UNITED STATES  
FOREIGN INTELLIGENCE SURVEILLANCE COURT  
WASHINGTON, D.C.

IN RE

NON-U.S. PERSONS

Docket No. 19-218

**OPINION**

On this date in the above-captioned docket, the Court granted a Verified Application (“App.”) for authorization to conduct electronic surveillance pursuant to Title I of the Foreign Intelligence Surveillance Act (FISA), codified as amended at 50 U.S.C. §§ 1801-1813. The targets of that application are non-U.S. persons believed by the Federal Bureau of Investigation (FBI) to be engaged in

in granting the application, the Court found, among other things, probable cause to believe that the targets are agents of a foreign power as defined at 50 U.S.C. § 1801(b)(2)(E) and that each of the facilities at which electronic surveillance will be directed is being used or are about to be used by the targets. In this Opinion the Court explains its reasoning regarding the latter finding.

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

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

## I. PROCEDURAL HISTORY

On December 12, 2018, the government submitted a draft application for authority to conduct electronic surveillance of the above-captioned targets. *See* Order at 1, No. 19-218 (FISA Ct. Mar. 27, 2019). The application discussed how the targets use [REDACTED]

[REDACTED] and described [REDACTED] as the facilities at which surveillance would be directed. Due to the complexity of the proposed surveillance and the issues presented, the Court appointed amici curiae with relevant legal and technical expertise – David Kris and Ben Johnson – on March 27 and 28, 2019. *See id.* at 2; Order at 2, No. 19-218 (FISA Ct. Mar. 28, 2019). The Court has benefitted greatly from the insights and expertise of both amici and is grateful for their contributions.

The government submitted a second draft application on March 29, 2019. On April 2, 2019, the Court held a meeting during which the Court and both amici asked questions and sought clarification from government representatives about the proposed surveillance and [REDACTED] used by the targets. In response to matters discussed during the April 2 meeting, the government filed another revised draft on May 7, 2019. The government submitted its Verified Application in final form on March 5, 2020.

## II. THE PROPOSED ELECTRONIC SURVEILLANCE

The [REDACTED] targets' use [REDACTED] central to this case. [REDACTED]

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

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

The

government believes that the targets use

in the United States, *see id.* at 10, 35, so there is reason to believe that some  
will be transmitted to or from the United States.

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

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

The government describes the facilities at which the proposed electronic surveillance will be directed as “facilities serviced by” [REDACTED] specified Internet [REDACTED] providers (“the providers”) “and denominated as . . . [REDACTED] *Id.* at 62 (emphasis in original). The government’s surveillance devices will be applied [REDACTED] within the United States. *Id.* at 52-53.

[REDACTED] which are set out in the Appendix to this Opinion. *Id.* at 41-43, 50-52.

*Id.* at 50-52. The government posits that the

[REDACTED] used by [REDACTED] targets. *Id.* at 44, 50-52.

### III. ANALYSIS

Pursuant to 50 U.S.C. § 1805(a)(2)(A), the Court has found probable cause to believe that the [REDACTED] targets<sup>1</sup> are agents of a foreign power [REDACTED] as defined at § 1801(b)(2)(E). Pursuant to § 1805(a)(2)(B), the Court has found probable cause to believe that each of the facilities at which the proposed electronic surveillance is directed is being used or is about to be used by a [REDACTED] target. With regard to the latter finding, the

---

<sup>1</sup> The target “is the individual or entity . . . about whom or from whom information is sought.” *See In re Sealed Case*, 310 F.3d 717, 740 (FISA Ct. Rev. 2002) (en banc) (quoting H. Rep. No. 95-1283, pt. 1, at 73 (1978)).

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

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

Court concluded: (1) [REDACTED] properly be regarded as “facilities” for purposes of § 1805(a)(2)(B); (2) the above-described electronic surveillance will be directed at [REDACTED]

[REDACTED] acquired by such surveillance; and (3) the facts and circumstances support a finding of probable cause to believe that each [REDACTED]

[REDACTED] at which such surveillance will be directed is being used, or is about to be used, by a [REDACTED]

[REDACTED] target. The Court explains the bases for those conclusions below.

A. [REDACTED] Properly Regarded as “Facilities” as that Term is Used in § 1805(a)(2)(B).

Title I of FISA contemplates that an electronic surveillance will be directed at one or more facilities or places. Specifically, an application for electronic surveillance “shall include,” among other things,

a statement of the facts and circumstances relied upon by the applicant to justify his belief 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.

§ 1804(a)(3)(B). A judge of the Foreign Intelligence Surveillance Court (FISC) may approve such an application upon finding, among other things, 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), and the resulting order

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

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

“shall specify,” among other things, “the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known,” § 1805(c)(1)(B).<sup>2</sup>

The legal amicus suggested that, for purposes of these provisions, the term “facilities” is best understood to refer to things [REDACTED] with which Congress was familiar and presumably had foremost in mind when it enacted FISA in 1978. From that premise, amicus argued for an interpretation of “facility” under which the Court should not regard something as a “facility” for purposes of § 1805(a)(2)(B) unless [REDACTED]. The amicus contended that, whenever plausibly supported by the facts, the Court should understand and analyze a proposed electronic surveillance as directed at [REDACTED] even if the government pleads the surveillance as directed at a different type of thing and that pleading is otherwise factually supported.

The Court understands that the amicus advanced this narrow interpretation of “facilities” out of concern that FISA should be applied with special caution in technological contexts that Congress could not foresee when it enacted the statute in 1978. But, as explained below, the Court concludes that Congress did not intend the term “facilities” in § 1805(a)(2)(B) to be interpreted in that narrow fashion. The Court therefore gives “facilities” its ordinary, broader meaning, which encompasses [REDACTED]

---

<sup>2</sup> If the nature and location are not known, the order must direct the government to inform the Court after it initiates electronic surveillance of a facility or place not specified in the order. See § 1805(c)(3).

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

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

The fundamental flaw in the amicus's suggested interpretation is that it lacks support in the statutory text. "In determining the meaning of a statutory provision, 'we look first to its language, giving the words used their ordinary meaning,'" *Lawson v. FMR LLC*, 571 U.S. 429, 440 (2014) (quoting *Moskal v. United States*, 498 U.S. 103, 108 (1990)), on "the assumption that the ordinary meaning of that language accurately expresses the legislative purpose," *Engine Mfrs. Ass'n v. South Coast Air Quality Mgmt. Dist.*, 541 U.S. 246, 253 (2004) (quoting *Park 'N Fly, Inc. v. Dollar Park & Fly, Inc.*, 469 U.S. 189, 194 (1985)). More precisely, a court generally looks to the ordinary meaning that a statutory term had when the provision in which it appears was enacted.<sup>3</sup> When Congress enacted the language at issue in 1978,<sup>4</sup> the term "facilities" was understood to denote the means used to facilitate an action or process.<sup>5</sup> [REDACTED] fit comfortably within that understanding of "facilities" because they are used to facilitate the

---

<sup>3</sup> See, e.g., *Wisconsin Central Ltd. v. United States*, 138 S. Ct. 2067, 2070-2071 (2018); *Sandifer v. United States Steel Corp.*, 571 U.S. 220, 227-28 (2014); *Perrin v. United States*, 444 U.S. 37, 42 (1979).

<sup>4</sup> Congress enacted the provisions now codified at 50 U.S.C. §§ 1804(a)(3)(B) and 1805(a)(2)(B) in 1978, see FISA, Pub. L. No. 95-511, §§ 104(a)(4)(B) and 105(a)(3)(B), 92 Stat. 1783, 1789-1790 (1978), and has not amended them.

<sup>5</sup> See *The American Heritage Dictionary of the English Language* 469 (new college ed. 1976) (defining facility in relevant part as "3. Often plural. The means used to facilitate an action or process; convenience; provision: *the facilities of a library.*") (emphasis in original). It now seems to have an even broader meaning in the telecommunications field. See *Newton's Telecom Dictionary* 518 (30<sup>th</sup> ed. 2016) (stating that "'facilities' means practically anything you want it to mean so long as it covers a sufficiently broad variety of 'things' which you haven't got a convenient name for").

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

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

communication

Moreover, the pertinent statutory provisions pair “facilities” with “places” to describe the things at which an electronic surveillance is directed. *See* §§ 1804(a)(3)(B), 1805(a)(2)(B) (“each of the facilities or places at which the electronic surveillance is directed”). The combination of those expansive terms is best understood to refer to any type of thing at which electronic surveillance can be directed, not to limit the types of things at which surveillance may be directed.

The use of the term “facilities” in other provisions of Title I of FISA does not support a more narrow interpretation. The term is used in a way that includes wires that transmit communications,<sup>6</sup> but it is also used to describe the obligations of third parties to furnish “all information, facilities, or technical assistance necessary to accomplish” an authorized electronic surveillance. § 1805(c)(2)(B). The manifest purpose of § 1805(c)(2)(B) is to secure necessary aid from third parties in conducting an authorized surveillance, which may not involve acquiring

---

<sup>6</sup> *See* 50 U.S.C. § 1801(l) (defining “wire communication” 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”) (emphasis added).

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

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

communications at all.<sup>7</sup> The narrow interpretation of “facilities” suggested by the amicus is at odds with the purpose of § 1805(c)(2)(B), which casts further doubt on its viability in the context of § 1805(a)(2)(B). *See, e.g., Henson v. Santander Consumer USA Inc.*, 137 S. Ct. 1718, 1723 (2017) (recognizing the “usual presumption that ‘identical words used in different parts of the same statute’ carry ‘the same meaning’”) (quoting *IBP, Inc. v. Alvarez*, 546 U.S. 21, 34 (2005)).

Accordingly, the Court affords the term “facilities” in § 1805(a)(2)(B) its ordinary, broad meaning, which includes [REDACTED]

B. The Proposed Electronic Surveillance will be Directed at [REDACTED]  
[REDACTED] Acquired by such Surveillance.

In pertinent part, FISA defines “electronic surveillance” as “*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 of any party thereto, if such acquisition occurs in the United States.*” 50 U.S.C. § 1801(f)(2) (emphasis added). That definition, and the related definitions of “contents”<sup>8</sup> and “wire communication,” were enacted in 1978, *see* FISA § 101(f), (l), (n), 92 Stat. at 1785-86, and have been amended only to exclude from the definition

---

<sup>7</sup> An electronic surveillance may consist of installing or using a surveillance device – *e.g.*, a camera – “for monitoring to acquire information, *other than from a wire or radio communication.*” 50 U.S.C. § 1801(f)(4) (emphasis added). And assistance in conducting an authorized surveillance may be compelled not only from a “communication or other common carrier,” but also from a “landlord, custodian or other . . . person.” § 1805(c)(2)(B).

<sup>8</sup> The definition of “contents” “includes any information concerning the identity of the parties to [a] communication or the existence, substance, purport, or meaning of that communication.” 50 U.S.C. § 1801(n).

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

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

of “electronic surveillance” the acquisition of certain communications of computer trespassers, *see* USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 1003, 115 Stat. 272, 392 (2001). Under the definition of electronic surveillance at § 1801(f)(2), “the electronic surveillance *is* the acquisition of the contents of communications.” [REDACTED]

No [REDACTED] Order & Mem. Op. at 8 (FISA Ct. Apr. 3, 2007) (emphasis in original) [REDACTED]

In this case, barring malfunction or error [REDACTED]

surveillance [REDACTED]

acquire [REDACTED]

only the contents of communication [REDACTED]

It is therefore sensible to say that the acquisition of the contents of communications, and by definition the surveillance itself, is *directed at* [REDACTED] *See The American Heritage Dictionary of the English Language* 373 (new college ed. 1976) (including in the definition of “direct” “To move (something or someone) toward a goal; aim; point.”). Importantly, that interpretive approach appropriately focuses the Court’s probable cause inquiry on the likelihood [REDACTED]

[REDACTED] subject to acquisition are being used by [REDACTED] target. Executive branch personnel will not be free “to direct surveillance against persons and communications of their unilateral choosing.” [REDACTED] Rather, as intended by Congress, “the pre-surveillance ‘judicial warrant procedure,’ and particularly the [REDACTED]

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

~~TOP SECRET//SI//ORCON/NOFORN/FIS~~

judge's probable cause findings, [will] provide an 'external check' on executive branch decisions to conduct surveillance." *Id.* at 14 (quoting S. Rep. 95-604, pt. 1, at 16 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3917).

The legal amicus, however, advanced a narrower understanding of when a surveillance is directed at a facility for purposes of § 1805(a)(2)(B). Following a line of analysis related to his suggested interpretation of "facilities," *see supra* pp. 6-9, he reasoned that Congress should be presumed to have had conventional telephone surveillance foremost in mind when in 1978 it enacted the provision now codified at § 1805(a)(2)(B). At that time, Congress would have understood that such surveillance is directed at telephone lines that are uniquely associated with a particular user or group of users to the exclusion of other persons. From that premise, the amicus concluded that § 1805(a)(2)(B) should be interpreted to *require* surveillance to be directed at a facility uniquely associated with a particular user or group of users.

On this point also, the language of § 1805(a)(2)(B) does not lend itself to the suggested interpretation. There is nothing in the phrase "facilities . . . at which the surveillance is directed" that indicates that the facilities must be uniquely associated with a particular user or group of users. By the terms of § 1805(a)(2)(B), the only required nexus between a facility at which surveillance will be directed and any person is probable cause to believe that the facility is being used or about to be used by a foreign power or an agent of a foreign power.<sup>9</sup>

---

<sup>9</sup> As discussed below, it is not necessary for the facility to be used *exclusively* by a foreign power or an agent of a foreign power. *See infra* p. 20.

~~TOP SECRET//SI//ORCON/NOFORN/FIS~~

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

The amicus argued that amendments to other parts of FISA – namely the specific selection term requirements for pen register/trap-and-trace (PR/TT) authorizations and orders to produce tangible things<sup>10</sup> and the limitation on acquiring “abouts” communications under Section 702 (codified at 50 U.S.C. § 1881a)<sup>11</sup> – support his interpretation of § 1805(a)(2)(B). But one would not usually expect recent acts of Congress to shed light on the meaning of statutory language enacted decades ago. At least as a general rule, “every statute’s *meaning* is fixed at the time of enactment,” even though “new *applications* may arise in light of changes in the world.” *Wisconsin Central Ltd.*, 138 S. Ct. at 2074 (emphasis in original). A court must have “an appropriate reason” to “depart from the original meaning of the statute,” *New Prime Inc. v. Oliveira*, 139 S. Ct. 532, 539 (2019), and speculation about how Congress *might* address new situations does not justify such departure.<sup>12</sup> As explained below, the Court does not find a sufficient basis to depart from its understanding of the original meaning of § 1805(a)(2)(B).

---

<sup>10</sup> See USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 103, 129 Stat. 268, 272 (2015) (codified at 50 U.S.C. § 1861(b)(2)(A) & (c)(2)(A), (3)); § 107, 129 Stat. at 273-74 (codified at § 1861(k)(4)); § 201, 129 Stat. at 277 (codified at 50 U.S.C. §§ 1841(4), 1842(c)(3)).

<sup>11</sup> See FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, § 103, 132 Stat. 3, 10-13 (2018) (codified in part at 50 U.S.C. § 1881a(b)).

<sup>12</sup> “[W]hile it is of course our job to apply faithfully the law Congress has written, it is never our job to rewrite a constitutionally valid statutory text under the banner of speculation about what Congress might have done had it faced a question that . . . it never faced.” *Henson*, 137 S. Ct. at 1725. See also *Magwood v. Patterson*, 561 U.S. 320, 334 (2010) (“We cannot replace the actual text with speculation as to Congress’ intent.”).

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

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

Pursuant to amendments enacted in 2015, *see supra* note 10, the government must identify a specific selection term to serve as the basis for using a PR/TT device, 50 U.S.C. § 1842(c)(3), or producing tangible things, § 1861(b)(2)(A). A specific selection term must “specifically identif[y] a person, account, address, or personal device, or any other specific identifier” and “limit, to the greatest extent reasonably practicable, the scope of [tangible things or PR/TT information] sought consistent with the purpose for seeking” them. §§ 1841(4)(A), 1861(k)(4)(A). Multiple terms or identifiers may be used to satisfy those requirements. §§ 1841(4)(D), 1861(k)(4)(A)(iii). By analogy, amicus reasoned that when [REDACTED] is used to describe the facilities at which electronic surveillance is directed, § 1805(a)(2)(B) should be interpreted to require [REDACTED] uniquely identify the users of those facilities.

The Court does not find the analogy instructive. Congress added the specific selection term requirements for types of collection which had merely required relevance to an investigation<sup>13</sup> in reaction to prior interpretations of relevance that it deemed unduly broad. *See* H. Rep. No. 114-109, pt. 1, at 18-19, 21 (2015). The relevance standard is lower than probable

---

<sup>13</sup> *See* § 1842(c)(2) (PR/TT application must include “a certification . . . that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities”); § 1861(b)(2)(B) (application for production of tangible things must include “a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities”).

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

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

cause and has no role in the Court's review of electronic surveillance applications under Title I of FISA. Therefore, the concerns that led Congress to adopt the specific selection term requirements in cases governed by the relevance standard have no bearing on this case.

Similarly, Congress adopted the "abouts" limitation in 2018, *see supra* note 11, in response to specific concerns. In March 2017, the National Security Agency (NSA) discontinued certain forms of Internet collection under Section 702 that had a heightened risk of acquiring non-pertinent information about U.S. persons. *See In re DNI/AG 702(h) Certification* [REDACTED] *Predecessor Certifications*, No. [REDACTED] *et al.*, Mem. Op. & Order at 12-14 (FISA Ct. Oct. 18, 2018). In addition to communications to or from a Section 702 target, the discontinued forms of Internet collection could acquire communications that were "about" a target, *i.e.*, ones to which the target was not a party, but which contained a reference to a facility used by the target, such as an email address. *Id.* at 12-13. In January 2018, Congress enacted the abouts limitation, which (absent narrowly defined exigent circumstances) imposed a requirement of congressional notification and a 30-day congressional review period before the government can resume abouts collection under Section 702. *Id.* at 10-11 (discussing FISA Amendments Reauthorization Act of 2017 § 103).

Here also, the particular concerns that led to enactment of the abouts limitation do not bear on the Title I electronic surveillance proposed in this case (which, of course, is not governed by Section 702). The proposed surveillance in this matter is designed to acquire [REDACTED] [REDACTED] to which a [REDACTED] target is a party, not abouts communications. And

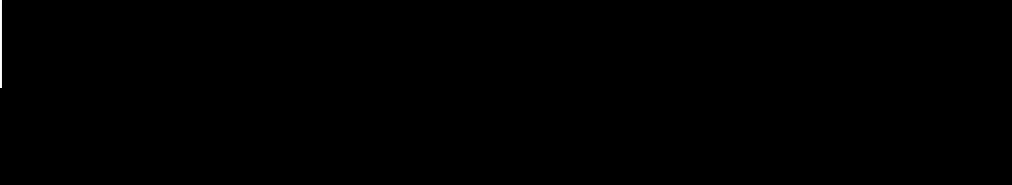
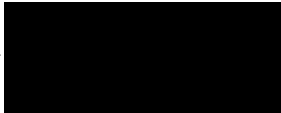
~~TOP SECRET//SI//ORCON//NOFORN/FISA~~

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

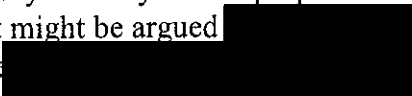
although the Court cannot rule out the possibility that non-target information may be acquired, *see infra* p. 19, there is no reason to expect substantial volumes of it will be acquired.

In sum, there is no tension between the specific selection term requirements and the abouts limitation, on one hand, and the Court's understanding of the original meaning of § 1805(a)(2)(B), on the other. Congress chose to respond to concerns that arose under other provisions of FISA by amending just those provisions, while leaving intact the statutory language that controls this case. And that language provides no basis for requiring that an electronic surveillance be directed at a facility that uniquely identifies a particular user or set of users.

Accordingly, the Court concludes that, for purposes of § 1805(a)(2)(B), the proposed surveillance is directed

  
 <sup>4</sup> The Court next considers whether, as required by that provision, there is probable cause to believe that each of those facilities is being used or about to be used by an agent of a foreign power, specifically, a  target.

---

<sup>14</sup> In view of the government's contention that it is exceptionally unlikely for the proposed surveillance to acquire non-target communications, *see infra* p. 19, it might be argued   
 to uniquely identify a particular set of users, *i.e.*, the  targets. For the reasons stated above, however, it is unnecessary to reach that question.

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

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

- C. There is Probable Cause to Believe that each [REDACTED] Proposed Electronic Surveillance is Directed is Being Used or About to be Used by a [REDACTED] Target.

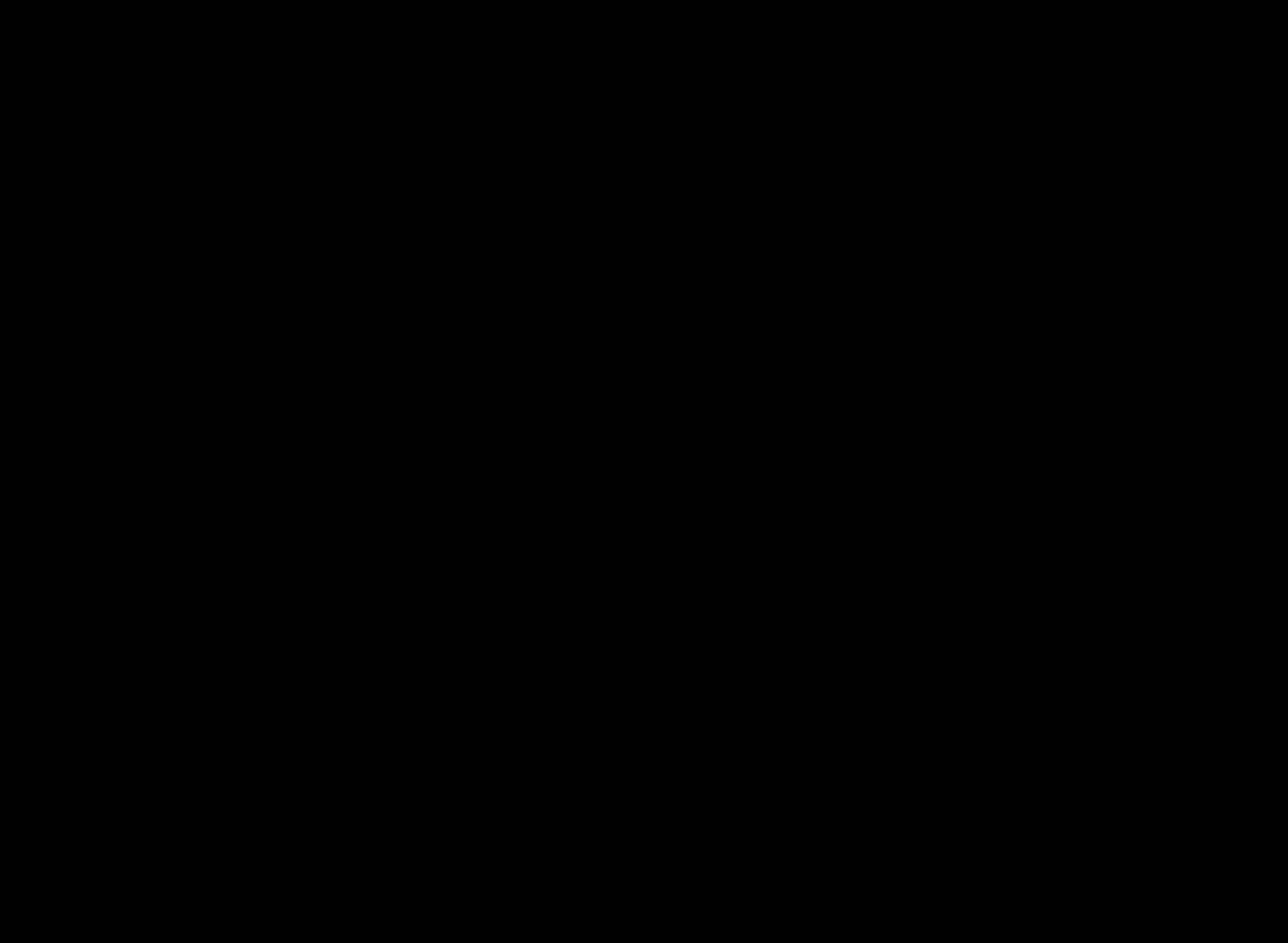
Probable cause is distinct from “[f]inely tuned standards such as proof beyond a reasonable doubt or by a preponderance of the evidence” and is “not readily, or even usefully, reduced to a neat set of legal rules.” *Illinois v. Gates*, 462 U.S. 213, 232, 235 (1983). It is a “practical and common-sensical standard,” the application of which calls for a “flexible, all-things-considered approach,” rather than “rigid rules, bright-line tests, and mechanistic inquiries.” *Florida v. Harris*, 568 U.S. 237, 244 (2013).

Probable cause takes its “substantive content from the particular contexts in which . . . [it is] being assessed.” *Ornelas v. United States*, 517 U.S. 690, 696 (1996). There is probable cause to conduct a law enforcement search “where the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found.” *Id.* That standard is satisfied when there is a “fair probability” of finding such evidence. *Harris*, 568 U.S. at 246 n.2; *Gates*, 462 U.S. at 238; *see also id.* at 244 n.13 (“[P]robable cause requires only a probability or substantial chance of criminal activity, not an actual showing of such activity.”).

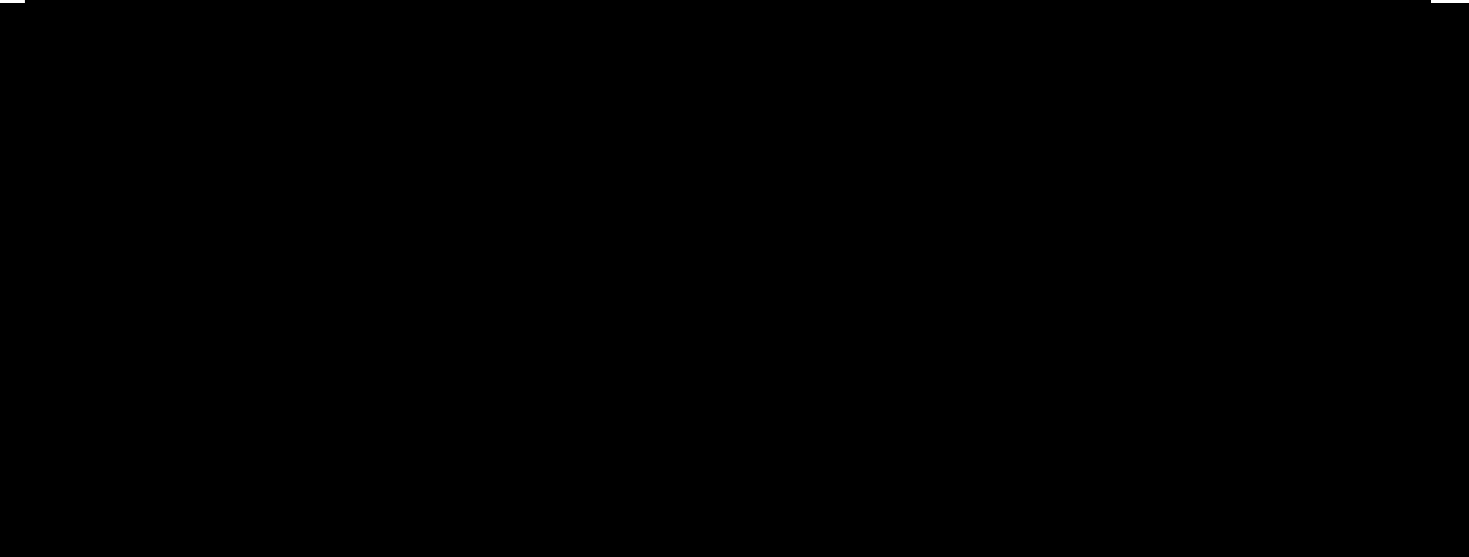
In this case, there is sufficient reason to believe that the [REDACTED] targets use [REDACTED]

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

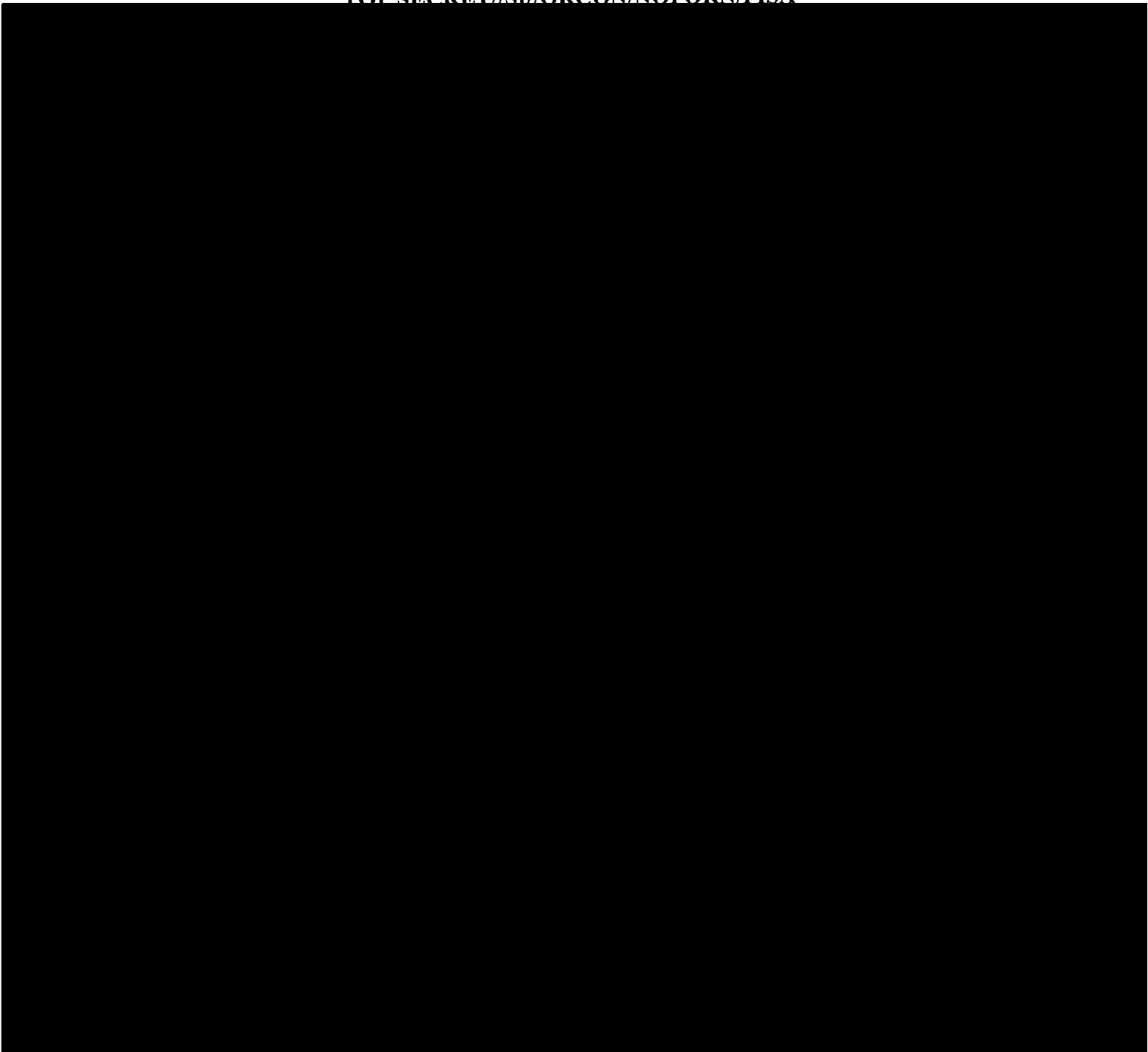
~~TOP SECRET//SI//ORCON/NOFORN/FISA~~



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



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



15



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

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

[REDACTED]

After examining the proffer and asking questions of government personnel, the technical amicus has not contested the government's contentions, nor has he recommended means of further tailoring the proposed surveillance to acquire only [REDACTED] communications. In the Court's assessment, the described facts and circumstances provide probable cause to believe that any particular communication [REDACTED] acquired by the proposed surveillance will [REDACTED] used by a [REDACTED] target.

It is possible, however, that the surveillance will acquire some [REDACTED] a [REDACTED] target is not a party. Such acquisitions could occur if [REDACTED] in a non-target communication [REDACTED]

Although "the FBI assesses that the likelihood of acquiring non-target communications is exceptionally low," *id.* at 49, such acquisitions cannot be ruled out.

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

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

A possibility – even a likelihood – that some non-target communications will be acquired need not foreclose approval of an electronic surveillance, if the minimization procedures adequately protect non-target U.S.-person information. 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.<sup>17</sup> The legal amicus has not suggested otherwise.

In shared-facility cases, non-target communications may be acquired because non-targets, *in addition to the target*, use the facility in question. In this case, non-target communications may be acquired because it is possible that surveillance will be directed at [REDACTED] [REDACTED] used by a non-target, *and not used by a target*. The Court now turns to how that possibility relates to assessing probable cause under § 1805(a)(2)(B). For the following reasons, the Court concludes that § 1805(a)(2)(B) does not require probable cause to believe that *all* [REDACTED] [REDACTED] which surveillance will be directed, without exception, are being used or about to be used by a [REDACTED] target. Rather, it suffices to find, as the Court has found,

---

<sup>17</sup> Here the minimization procedures in this case afford sufficient protection.

[REDACTED]

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

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

probable cause to believe that *each* [REDACTED] which surveillance will be directed is being used or about to be used by a [REDACTED] target.<sup>18</sup>

That interpretation squares with the text of § 1805(a)(2)(B). The word “each” is used as a pronoun in that provision. When so used, “each” is defined as “[e]very one of a group of objects, persons, or things considered individually; each one.” *The American Heritage Dictionary of the English Language* 408 (new college ed. 1976). Thus, it is consistent with the language of § 1805(a)(2)(B) to determine whether there is probable cause to believe that each one of the facilities, considered individually, is being used or about to be used by an agent of a foreign power, without further inquiring whether there is probable cause to believe that they are all, without exception, being used or about to be used by such an agent.

An example may clarify the distinction between those two formulations. Suppose that the government submits an application for electronic surveillance of Jones, which establishes probable cause to believe that he is an agent of a foreign power. The application seeks approval of electronic surveillance of three cell phone numbers and provides information regarding Jones’s asserted use of those numbers. Under the Court’s interpretation of § 1805(a)(2)(B), the judge reviewing the application would make a probable cause determination regarding Jones’s

---

<sup>18</sup> In view of the government’s assertion that acquiring non-target communications is exceptionally unlikely, *see App.* at 49, there might be a sufficient basis for finding probable cause to believe that all [REDACTED] which surveillance will be directed, without exception, are being used or about to be used by the targets. That question would be clearer if there were more information about [REDACTED]. In any case, the Court finds that inquiry unnecessary for the reasons stated herein.

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

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

use of the first cell phone number, another determination regarding use of the second number, and another regarding use of the third. After making such a determination for each number, considered individually, the judge's work under § 1805(a)(2)(B) would be done. The judge would not assess whether there is probable cause to believe that Jones is using or about to use all three numbers, without exception.

In the experience of the undersigned judge, that interpretation comports with how FISC judges routinely apply § 1805(a)(2)(B). For example, in [REDACTED]

[REDACTED] No. 19- [REDACTED] Primary Order at 9 (FISA Ct.

March 20, 2019) [REDACTED], the undersigned judge approved electronic surveillance of [REDACTED]

[REDACTED] The Court made the probable cause findings in that case because there was

sufficient reason to believe that each [REDACTED]

[REDACTED] was being used or about to be used by the target. The Court did not inquire whether there was probable cause to believe that *all* [REDACTED] without exception, were being used or about to be used by the target.

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

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

Moreover, because the probable cause standard requires only a fair probability, *see supra* p. 16, 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. *See Harris*, 568 U.S. at 249 (“[W]e do not evaluate probable cause in hindsight, based on what a search does or does not turn up.”). A requirement of probable cause to believe that a target uses all facilities at which surveillance is to be directed, without exception, would require a higher level of confidence regarding use of each facility than is usually required for probable cause. That is because, even for a small number of facilities, a fairly strong probability that each facility is used by a target may correlate with a much lower probability that the target uses all of them.

More fundamentally, it would be illogical for approval of surveillance of one facility to depend on the likelihood that the target uses a different facility. But that is the result of interpreting § 1805(a)(2) to require probable cause to believe that the target is using or about to use *all* facilities at which surveillance will be directed. The government could try to unbundle the facilities for probable cause purposes by bringing a separate application for each one, but it would be unclear, to say the least, why the bar for probable cause should be raised or lowered depending on procedural form.

To be sure, this case does not present all of the considerations discussed above. Here the facilities at which surveillance will be directed are described by

The government makes the same proffer for all such facilities and they cannot be separately pled and targeted without altering the manner in

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

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

which the surveillance would be conducted. But § 1805(a)(2)(B) must be given a single consistent interpretation, even if the case *sub judice* does not present all of the considerations that lead a court to adopt that interpretation. For example, in *Clark v. Martinez*, 543 U.S. 371 (2005), the Supreme Court interpreted a statute to avoid constitutional difficulties as applied to one class of aliens, even though the case before it did not present those difficulties because it involved a different class. The Court observed that “[t]o give these same words a different meaning for each category [of alien] would be to invent a statute rather than interpret one,” and rejected a “novel interpretive approach . . . which would render every statute a chameleon, its meaning subject to change depending on the presence or absence of constitutional concerns in each individual case.” *Id.* at 378, 382.<sup>19</sup>

Interpreting § 1805(a)(2)(B) to require probable cause to believe that, considered individually, each facility at which the surveillance will be directed is being used or about to be used by a foreign power or an agent of a foreign power comports with the statutory text and the nature of the probable cause standard. An alternative interpretation, under which there must be probable cause to believe that all such facilities, without exception, are being used or about to be

---

<sup>19</sup> See also *United States v. Santos*, 553 U.S. 507, 522 (2008) (Scalia, J., joined by two justices) (refusing to give “the same word, *in the same statutory provision*, different meanings *in different factual contexts*”) (emphasis in original), *superseded by statute*, Fraud Enforcement and Recovery Act of 2009, Pub. L. No. 111-21, § 2(f), 123 Stat. 1617, 1618 (2009); *id.* at 532, 546 (Alito, J., dissenting, joined by three justices) (rejecting interpretation under which meaning of term varies depending on the facts presented); *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004) (“Because we must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context, the rule of lenity applies” in noncriminal case); *United States v. Thompson/Center Arms Co.*, 504 U.S. 505, 517-18 & n.10 (1992) (plurality opinion) (statute cannot be interpreted differently in civil and criminal cases).

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

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

used by such a target would lead to anomalous results in many cases. Accordingly, the Court adopts the former interpretation, pursuant to which it has made the probable cause finding required by § 1805(a)(2)(B) in this case.

As always, the Court has assessed probable cause based on the facts before it. The results of the authorized surveillance may weaken or strengthen the basis for probable cause if the government brings a renewal application. The Court is ordering the government by the end of the authorized surveillance period to report the number of communications acquired and how many of those communications are assessed to be non-target communications. *See* Primary Order at 9-10. For each non-target communication, the government must (a) report the location and U.S.-person status of the parties, if known; (b) assess how and why the communication was acquired; and (c) describe its handling and disposition. *Id.* at 9. That information is expected to assist the Court in assessing the probable cause and minimization issues presented by any renewal application.

#### IV. CONCLUSION

For the foregoing reasons, the Court made the probable cause findings required by 50 U.S.C. § 1805(a)(2)(B). Having found the other applicable requirements satisfied as well, the Court approved the proposed electronic surveillance.

ENTERED this 5<sup>th</sup> day of March, 2020.

  
ROSEMARY M. COLLYER  
Judge, United States Foreign  
Intelligence Surveillance Court

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

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

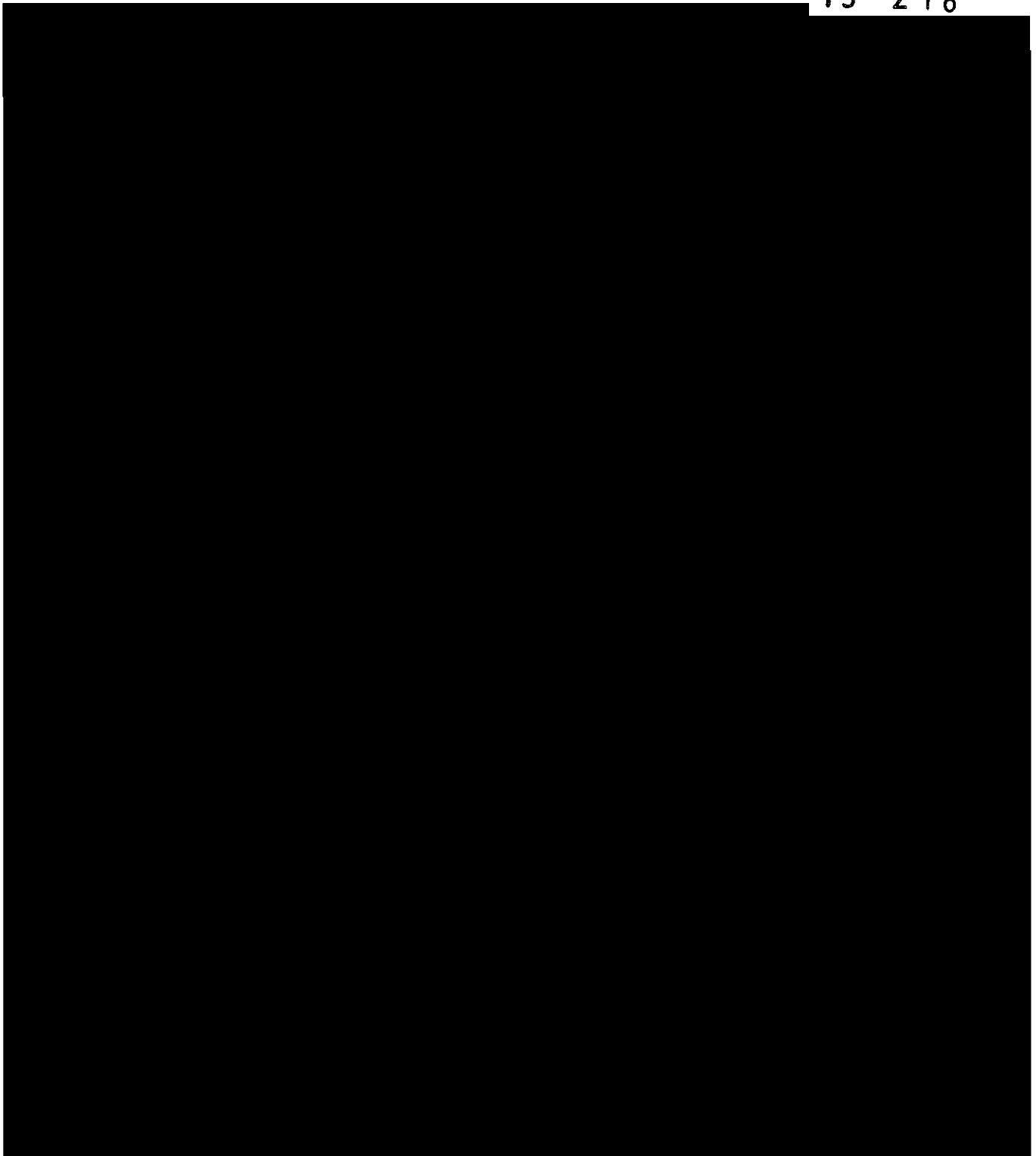
MAR 05 2020

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

LeeAnn Flynn Hall, Clerk of Court

APPENDIX

19 - 218



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