~~SECRET~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

b6
b7C

(S)

Docket Number:

b1
b3
b7E

**MEMORANDUM OF LAW IN RESPONSE TO THE COURT'S ORDER REGARDING UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT**

b7E

The United States submits this Memorandum of Law in response to this Court's Order, directing the government to explain how, if at all,

b7E

under the Foreign Intelligence Surveillance Act of 1978, as amended, Title 50 United States Code (U.S.C.), § 1801, et seq. (FISA). As a threshold matter, interpreting

~~SECRET~~

Classified by: James A. Baker, Counsel for Intelligence Policy, OIPR, DOJ
Reason: 1.4(c)
Declassify on: X1

criminal statutes is not controlling on this Court. Moreover, as described more fully below, because [redacted] b7E [redacted] both the plain meaning and legislative history of the criminal pen register statute and misapplied certain canons of statutory construction, the government respectfully submits that this Court should decline to follow [redacted] In addition, the 2006 USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 506, 120, Stat. 192, 248 (2006), which enhanced the government's ability to obtain certain routing and transmission information pursuant to pen register surveillance under FISA, provides additional authority that was not applicable in the [redacted] under which the government can obtain [redacted] b7E [redacted] (U)

The government further submits that both the plain text of the criminal pen register statute and its legislative history confirm that the government is authorized [redacted] b7E [redacted] As explained more fully below, Congress has repeatedly recognized that [redacted]

[redacted] Accordingly, it has b7E

enacted a pen register statute [redacted]

[redacted] which reaches the untenable

result that the government must forego [redacted]

[redacted]

## I. BACKGROUND (U)

[redacted] (S)

b1
b3
b7E

[1] As stated in the government's Verified Memorandum, [redacted] b7E

[redacted] (S)

b1
b3
b7E

[redacted] (S)

b1
b3
b7E

[redacted]

b7E

[2] As explained in the government's Verified Memorandum, FISA authorizes the Court to issue orders approving the installation and use of pen registers and provides that "the term[] 'pen register' . . . ha[s] the meaning[] given such term[] in Section 3127 of Title 18, United States Code." 50 U.S.C. § 1841(2). Section 3121(c) applies in the FISA context because FISA pen registers are authorized under "this chapter," i.e., Chapter 206 of Title 18, 18 U.S.C. § 3121(a). Verified Memorandum at 6, 9. (U)

[redacted] (S)

b1
b3
b7E

Shortly after the government filed its Verified Memorandum,

[redacted]

b7E

[redacted] (S)

b1
b3
b7E

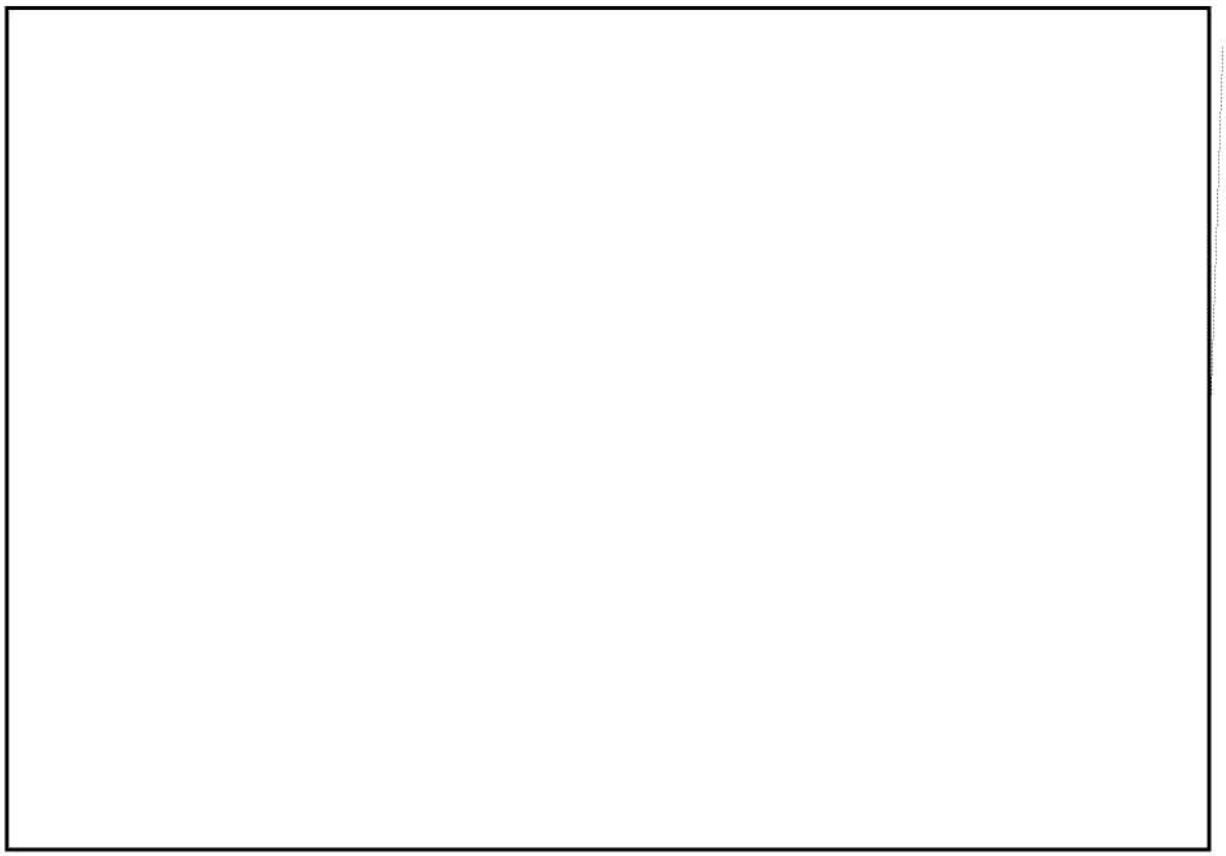
[redacted] b7E

In support of its application, the government asserted that 18 U.S.C. §§ 3127(3) and 3121(c) authorize the government to collect [redacted] rejected this argument and determined that [redacted]

[redacted] b1 b3 b7E (S)

2. This Memorandum responds to that Order. ~~(S)~~ (U)

~~SECRET~~



(S) b1 b3 b7E

[4] See, e.g., Brightpoint, Inc. v. Zurich American Ins. Co., 2006 WL 69337, slip op. at *6 (S.D.N.Y. Mar. 10, 2006)(noting that a federal district court opinion from another district had no precedential value); PFS Investments, Inc. v. Poole, 2006 WL 13025, slip op. at *2, n. 2 (W.D.N.C. Jan. 3, 2006) (stating that one district court is not bound by the decisions of other district courts). (U)

~~SECRET~~

## II. ARGUMENT (U)

### A. The Plain Text of the Criminal Pen Register Statute and FISA Authorize the Government Incidentally [redacted] (U)

b7E

#### 1. The Text of 18 U.S.C. § 3127(3) (U)

Congress initially adopted the definition of "pen register" in 1986 as part of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 302, 100 Stat. 1848, (ECPA). As originally enacted, 18 U.S.C. § 3127(3) defined pen register in terms of now out-dated telephone technology, referring to a "device" being attached to a "telephone line." Specifically, the earlier version of the pen register definition provided as follows:

> [T]he term "pen register" means a device which records or decodes electronic or other impulses which identify the number dialed or otherwise transmitted on the telephone line to which such device is attached, . . . ."

18 U.S.C. § 3127(3) (2000). This definition remained unchanged until 2001, when Congress amended it in the USA PATRIOT Act, to clarify that the pen register provision applies to an array of modern communications technologies (*e.g.*, the Internet) and not simply traditional telephone lines. See H.R. REP. No. 107-236(I), at 52-53 (2001); see also 147 CONG. REC. S11,005-S11,014, S11,006 (daily ed. Oct. 25, 2001)(section-by-section analysis by

Sen. Leahy). The current definition of pen register now states, in pertinent part, as follows:

> the term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication . . . .

18 U.S.C. § 3127(3) (emphasis added). Thus, Congress amended the pen register definition in only two respects, both of which merely clarified the limits of existing law: (1) Congress broadened the language to include the recording or decoding of "dialing, routing, addressing or signaling information" in order to confirm the statute's proper application to tracing communications in an advanced electronic environment; and (2) Congress confirmed the proper purpose and scope of a pen register device: to obtain information used to process a wire or electronic communication, but not to obtain the "contents" of such communication. (U)

On their face, neither the original version of this definition nor the revised version as amended by the USA PATRIOT Act dictates the means by which a pen register device should function technologically. By its own terms, this provision is simply a definition. (Section 3127 is entitled "Definitions for Chapter"). [redacted] b7E

[redacted] b7E

[redacted] As discussed below, it is 18 U.S.C. § 3121, not § 3127, that sets forth the "general prohibition on pen register and trap and trace device use." [redacted] (U)

Importantly, in amending 18 U.S.C. § 3127(3), Congress clearly intended that through a pen register device, the government can lawfully obtain all non-content information -- "dialing, routing, addressing, or signaling information" -- transmitted by a targeted telephone. [redacted] b7E

[redacted] Without such [redacted] b7E

the purpose of a telephone pen register -- [redacted]

[redacted] (U)

2 [redacted] b1 b3 b7E (S)

[redacted] b1 b3 b7E (S)

An order issued under this section . . .

[redacted] b7E

[redacted] b7E

[redacted] b7E

(U)

[redacted] (S) b1 b3 b7E

[redacted] (S)

b1
b3
b7E

### 3. The Text of 18 U.S.C. § 3121(c) (U)

Congress first added the "limitation" section of the pen register statute, 18 U.S.C. § 3121(c), in 1994 as an amendment to the Communications Assistance for Law Enforcement Act, Pub. L. 103-414, 108 Stat. 4279 (1994) (CALEA). As originally enacted, that provision stated as follows:

> (c) Limitation - A Government agency authorized to install and use a pen register under this chapter or under state law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing.

CALEA, § 207, 108 Stat. 4292 (emphasis added). The plain text of this provision required the government to use, in pen register devices, "technology reasonably available to it" in order to "restrict[] the recording or decoding" to "dialing and signaling information" (i.e. digits) "utilized" to connect calls. [redacted]

b7E

[redacted]

[redacted] b7E

[redacted] Indeed, as discussed more fully below, any other reading of this provision would render the words "reasonably available to it" superfluous in violation of the simple rule of statutory construction that all words of a statute be given meaning, if possible. See TRW, Inc. v. Andrews, 534 U.S. 19, 31 (2001) (citation omitted) ("It is a cardinal principal of statutory construction that, if it can be prevented, no clause, sentence, or word shall be superfluous, void or insignificant.") Courts must strive to "give effect, if possible, to every clause and word of a statute." Id. (citation omitted). Congress deliberately chose to make [redacted] b7E

[redacted] (U)

In the 2001 USA PATRIOT Act, Congress also amended the limitation provision in 18 U.S.C. § 3121(c) (1994) to conform to the revised language of the pen register definition. In fact, Congress made the same revisions to the limitation provision that it made to the pen register definition: (1) it clarified that the term "pen register" applies not only to traditional telephone lines, but to all manner of modern electronic communications; and (2) it clarified that the purpose of a pen register is to collect

call processing information, [redacted] b7E

[redacted]

18 U.S.C. § 3121(c) (emphasis added). [redacted]

[redacted] b7E

This amendment changed nothing about the permissible use of a pen register. As was true before the USA PATRIOT Act, [redacted]

**B. The Legislative History of the Pen Register Provisions** [redacted] (U)

b7E

**1. 1994 Legislative History Regarding 18 U.S.C. § 3121(c) Confirms that Congress Intentionally Created a Technology-Driven Minimization Scheme (U)**

In his opinion, [redacted] cited hearing testimony from the 1994 congressional deliberations on CALEA, legislative history from the USA PATRIOT Act and secondary sources, asserting that the government's "fundamental premise" that 18 U.S.C. § 3121(c) [redacted] He ignored, however, critical legislative history from the 1994 enactment of the pen register [redacted] As discussed below, that history confirms what the text of 18 U.S.C. § 3121(c) plainly implies. (U)

b7E

b7E

In 1994, Senator Leahy originally proposed 18 U.S.C. § 3121(c) as part of S.2375, the "Digital Telephony Act of 1994." See 140 CONG. REC. 20,4444 (1994). Most of the provisions of S.2375, including 18 U.S.C. § 3121(c), were eventually adopted in CALEA. [redacted]

b7E

[redacted] b7E

[redacted] Thus, Senator Leahy, the primary architect of 18 U.S.C. § 3121(c), stated that the government was required to [redacted] b7E

[redacted]

In addition to Senator Leahy's statement, committee reports from both the House and Senate further confirm that Congress originally intended to permit the government [redacted] b7E

[redacted]

[redacted] b7E

[redacted] b7E

[redacted] Well in advance of the 1994 enactment of this provision, [redacted] both Title III, enacted in 1968, and FISA, enacted in 1978. (U)

For example, 18 U.S.C. § 2518(5) of Title III provides, in relevant part, that electronic surveillance "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception" under Title III. Under well-established precedent, Title III "does not forbid the interception of all non-relevant conversations, but, rather, instructs the [government] to conduct the surveillance in such a manner as to minimize the interception of such conversations." Scott v. United States, 436 U.S. 128, 140 (1978) (emphasis omitted). (U)

Similarly, under FISA, each application for electronic surveillance submitted by the government must contain, among other things, [redacted] b7E [redacted] 50 U.S.C. § 1804(a)(5). FISA defines "minimization procedures," in part, as follows:

> specific procedures, . . . that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and

> retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

50 U.S.C. § 1801(h)(1). Both federal case law and FISA legislative history demonstrate that the definition of minimization procedures under FISA was intended to take into account the realities of foreign intelligence collection, where the activities of individuals engaged in clandestine intelligence or international terrorism are often not obvious on their face, and an investigation develops over time. See, e.g., United States v. Rahman, 861 F. Supp. 247, 253 (S.D.N.Y. 1994), aff'd on other grounds, 189 F.3d 88 (2d Cir. 1999) (rejecting the notion that the "wheat" could be separated from the "chaff" while the "stalks were still growing"). b7E

When drafting 18 U.S.C. § 3121(c) and its associated legislative history, Congress undoubtedly knew the legal meaning that the term "minimize" had acquired under Title III and FISA, electronic surveillance laws that had, at the time, existed for nearly three decades. In any event, Congress is presumed, as a matter of law, to have known the legal meaning of that word. See United States v. Bonanno Organized Crime Family, 879 F.2d 20, 25 (2d Cir. 1989) relying on Goodyear Atomic Corp v. Miller, 486 U.S. 174, 184-185 (1988) (As a matter of law, Congress is presumed to have been (a) knowledgeable about existing laws pertinent to later-enacted legislation, (b) aware of judicial interpretations given to sections of an old law incorporated into a new one, and (c) familiar with previous interpretations of specific statutory language).

[redacted] b7E

[redacted] b7E

c. The USA PATRIOT Act Legislative History Confirms that Congress [redacted] b7E (U)

According to [redacted] when Congress first codified the pen register law under ECPA, it did not address the question of [redacted] b7E

[redacted] In fact, the USA PATRIOT Act legislative history, though scant, proves just the opposite: [redacted] b7E

Nowhere in the legislative history of the USA PATRIOT Act did Congress suggest that the amendments to 18 U.S.C. §§ 3121(c) and 3127(3) were intended [redacted] b7E

[redacted]

Specifically, although the USA PATRIOT Act contains no definitive Congressional committee report, on October 11, 2001, the House Judiciary Committee reported on a predecessor bill, H.R. 2975, that proposed updating the language of sections 3127(3) and 3121(c) to confirm that pen registers apply to communications instruments other than traditional telephones. b7E

[redacted]

b7E

b7E

On October 25, 2001, Senator Leahy, the chairman of the Senate Judiciary Committee, appeared before the Senate and read final remarks about the USA PATRIOT Act, which were published in the Congressional Record. Senator Leahy's section-by-section analysis of the Senate bill was also published in the record.

b7E

[redacted] b7E

[redacted] b7E

[redacted] has taken portions of Senator Leahy's remarks and used them out of context. In fact, Senator Leahy stated that his original proposal for the USA PATRIOT Act amendments to the pen register statute was threefold: (1) to give nationwide effect to pen register and trap and trace orders obtained by government attorneys and obviate the need to obtain identical orders in multiple federal jurisdictions; (2) to clarify that such devices can be used for computer transmissions to obtain electronic addresses, not just telephone lines; and (3) "as a guard against abuse," to provide for "meaningful judicial review of government attorney applications for pen registers and trap and trace devices." 147 CONG. REC. S10,990-S11,060, S10,999. Senator

Leahy's third proposal was not adopted in the USA PATRIOT Act,

[redacted] b7E

In short, Senator Leahy had proposed that the criminal pen register application process should be subjected to heightened judicial review. Id. at S11000. Currently, under the criminal pen register statute, the government must certify that the information likely to be obtained by the installation of a pen register device will be "relevant to an ongoing criminal investigation." Id. A court is required to issue an order upon seeing the certification and is not authorized to look behind the certification and evaluate the judgment of the prosecutor. Senator Leahy sought to amend this standard to require the government to include facts in its pen register certification. Id. Then, the court would grant the order only if it found that the facts supported the government's assertion of relevancy.

[redacted] b7E

[redacted] b7E

[redacted] heightened judicial review of the applications was necessary to ensure that the government was properly using pen register orders. Id. A majority of Congress apparently did not agree with him, because this proposed amendment did not become law. (U)

[redacted]

[redacted] He was b7E referring instead to his proposed amendment to the legal standard applicable to a pen register order. Id. As stated above, that amendment was not adopted. Senator Leahy hoped to amend the criminal pen register statute to require judicial review of the facts asserted in support of a pen register application, [redacted] b7E

[redacted] The Senator did not claim that under his proposed approach or as amended by the USA PATRIOT Act the criminal pen register statute would eliminate, or even curtail,

the acknowledged status quo under which pen register devices capture all electronic impulses, non-content or otherwise, from the targeted facility. Had he believed that either his approach or the amended statute would have done so, he could have stated as much. In sum, [redacted] argument that the USA PATRIOT Act amendments [redacted] (U)

b7E

D. [redacted] **has Misapplied Canons of Statutory Construction** (U)

b7E

**1. No Clause or Words Should be Rendered Superfluous** (U)

b7E

[redacted]

b7E

Despite [redacted] the statute is not silent on the possibility that the technology may not exist. In fact, the provision expressly recognizes the government's technological limitations. Hence, it requires the use of only technology "reasonably available" to the government. [redacted] conclusion that Congress "assumed" that technology would exist is not supported by the record. [redacted]

b7E

[redacted] seemed inadvertently to acknowledge that his interpretation voids the words "reasonably available." [redacted]

**2. The Two Related Provisions of the Pen Register Statute Must be Read in Harmony (U)**

[redacted] also rejected the government's contention that allowing [redacted] b7E [redacted] 18 U.S.C. § 3127(3) with 18 U.S.C. § 3121(c). He reduced the government's interpretation to the maxim, [redacted] While he acknowledged that this is "one possible way to read § 3121(c)," he dismissed this view, concluding that the government must [redacted] concluded that his is the only reading that harmonizes the two sections, [redacted] (U)

[redacted] b7E

[redacted] The [redacted] ruling, [redacted] Nor is it consistent with the legislative history which acknowledges the technological constraints, [redacted]

[redacted] b7E

[redacted] Nor, as described above, is it consistent with long-standing judicial interpretations of the minimization requirements of Title III and FISA. Also, as noted above, this position would be particularly inconsistent under FISA in light of the USA PATRIOT Reauthorization Act amendments [redacted]

(U)

**3. The Cannon of Constitutional Avoidance** (U)

At the conclusion of his opinion, [redacted] invoked the doctrine of constitutional avoidance, which, he stated, "compels a court to construe a statute in a manner which avoids serious constitutional problems, unless such a construction is plainly contrary to the intent of Congress." Id. at *18. [redacted] b7E

[redacted] He determined that his interpretation of the statute, which bans the government from

[redacted] b7E

The government submits that [redacted] misapplied the canon of constitutional avoidance. That canon provides that "if an otherwise acceptable construction of a statute would raise serious constitutional problems, and where an alternative interpretation of the statute is 'fairly possible,' [the court] is obligated to construe the statute to avoid such problems." INS v. St. Cyr, 533 U.S. 289, 299-300 (2001)(citations omitted). In his opinion, [redacted] directly proceeded to the constitutional question of "warrantless surveillance" without giving effect to Congress's expressed intent to itself avoid Fourth Amendment problems by [redacted] b7E (U)

The canon of constitutional avoidance does not allow the court to overlook the plain text of the statute and thereby

disregard Congressional intent and Congress's scheme for addressing possible Fourth Amendment issues [redacted] b7E

[redacted] Rather, the canon is "a tool for choosing between competing plausible interpretations of a statutory text, resting on the reasonable presumption that Congress did not intend the alternative which raises serious constitutional doubts." Clark v. Martines, 543 U.S. 371, 381, 125 S.Ct. 716 (2005). "The canon is thus a means of giving effect to congressional intent, not of subverting it." Id. (U)

In addition, the legal basis underpinning [redacted] b7E application of the doctrine of constitutional avoidance - [redacted] The Court stated, "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is not a question presented by this case." Katz, 389 U.S. at 358. Furthermore, no other federal court has ever held that the Fourth Amendment warrant requirement applies

to cases involving foreign powers or agents of foreign powers. See House Report 95-1283, Pt. I at 17-21.

b7E

(U)

4.

b7E

The government submits that the scheme adopted by Congress in 18 U.S.C. §§ 3127(3) and 3121(c),

b7E

The Fourth Amendment prohibits "unreasonable searches and seizures" and directs that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be search, and the persons or things to be seized." U.S. Const. amend. IV. The touchstone for review of government action under the Fourth Amendment is whether a search is "reasonable." See, e.g., Veronia Sch. Dist. v. Acton, 515 U.S. 646, 653 (1995). Under the FISA pen register provision, the

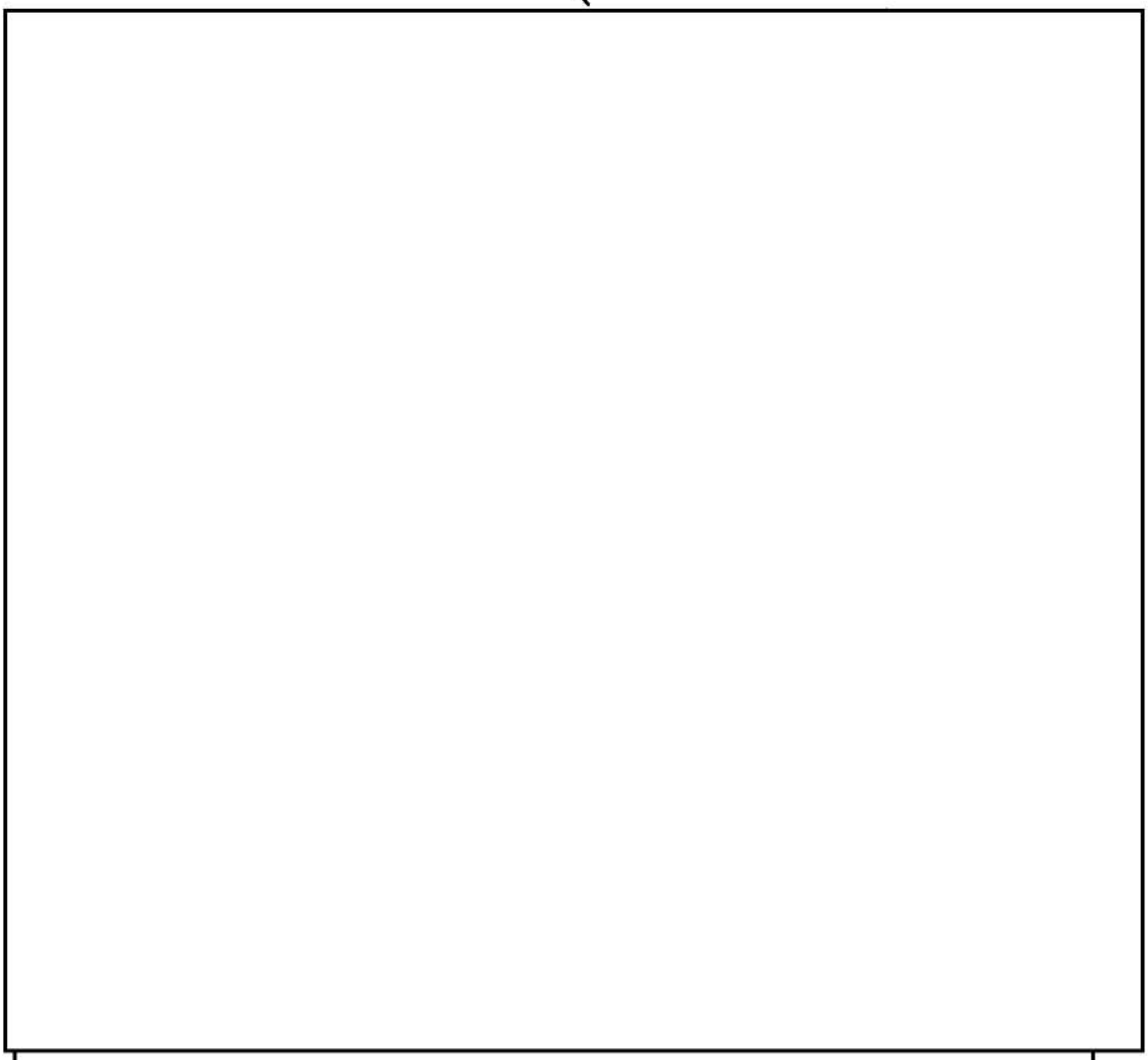
government can only obtain authority to install and use such devices for investigations to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities. For purposes of pen register surveillance under FISA, [redacted] b7E

[redacted]. (U)

Reasonableness, in this context, must be assessed under a general balancing approach, "'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of a legitimate government interest.'" United States v. Knights, 534 U.S. 112, 118-19 (2001) (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)). [redacted] b7E

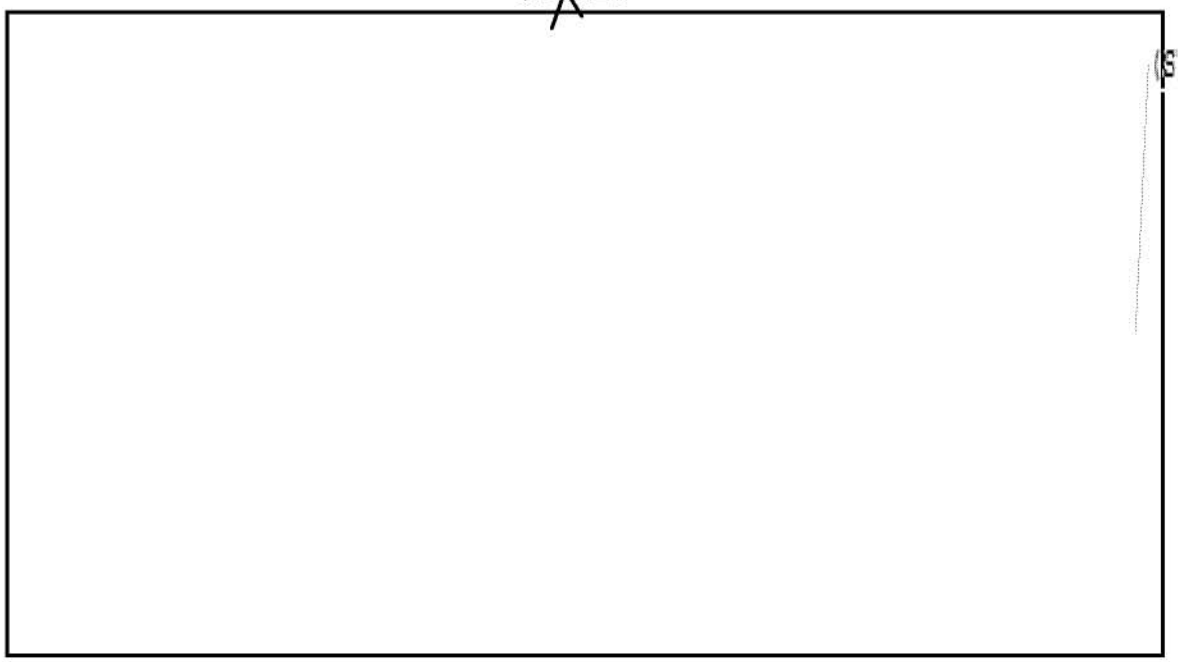
[redacted]

b7E



b1
b3
b7E

(S)



(S)

b1
b3
b7E

Moreover, emergency exceptions to warrantless surveillance have been long recognized as a matter of statute (under both FISA and the criminal code) and as a matter of Fourth Amendment case law. See, e.g., 50 U.S.C. § 1804(f) (allowing the Attorney General to authorize emergency employment of electronic surveillance when the Attorney General reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained); 18 U.S.C. § 2518(7) (allowing certain high-ranking Justice Department officials to authorize emergency surveillance if a situation exists that involves

immediate danger of death or serious physical injury to any person, conspiratorial activities threatening the national security or conspiratorial activities characteristic of organized crime); Mincey v. Arizona, 437 U.S. 385, 393-394 (1978) ("[W]arrants are generally required to search a person's home or his person unless the 'exigencies of the situation' make the needs of law enforcement so compelling that the warrantless search is objectively reasonable under the Fourth Amendment") (citation omitted). (U)

b1
b3
b7E

[redacted] (S)

//

//

//

//

## III. CONCLUSION (U)

(S) [redacted] b1 b3 b7E

Respectfully submitted,

James A. Baker
Counsel for Intelligence Policy
United States Department of Justice

[redacted]
Associate Counsel

[redacted]
Senior Attorney

Office of Intelligence Policy and Review
United States Department of Justice