Approved for public release by the ODNI 20160818

Filed
United States
Foreign Intelligence Surveillance
Court of Review

APR 14 2016

LeeAnn Flynn Hall, Clerk of Court

United States Foreign Intelligence Surveillance Court of Review

IN RE: CERTIFIED QUESTION OF LAW

Docket No. FISCR 16-01

Upon Certification for Review by the United States Foreign Intelligence Surveillance Court

Decided:

MARC ZWILLINGER, ZwillGen PLLC, Washington, D.C., argued the case as court-appointed amicus curiae. With him on the brief was JACOB A. SOMMER.

ADITYA BAMZAI, United States Department of Justice, Washington, D.C., argued the case for the United States. With him on the brief were JOHN P. CARLIN, STUART J. EVANS, J. BRADFORD WIEGMANN, AND LISA M. FARABEE.

Before BRYSON, CABRANES, AND TALLMAN, *Judges*.

PER CURIAM.

The Foreign Intelligence Surveillance Court ("FISC") certified this matter under 50 U.S.C. § 1803(j) for review by this court. The FISC certified the following question to us:

Whether an order issued under 50 U.S.C. § 1842 may authorize the Government to obtain all post-cut-through

Approved for public release by the ODNI 20160818

digits, subject to a prohibition on the affirmative investigative use of any contents thereby acquired, when there is no technology reasonably available to the Government that would permit:

(1) a PR/TT [pen register/trap-and-trace] device to acquire post-cut-through digits that are non-content DRAS [dialing, routing, addressing, and signaling] information, while not acquiring post-cut-through digits that are contents of a communication; or

(2) the Government at the time it receives information acquired by a PR/TT device, to discard post-cut-through digits that are contents of a communication, while retaining those digits that are non-content DRAS information.

We have reviewed the record and considered briefs from the government and from amicus curiae appointed by the court under 50 U.S.C. § 1803(i) to present argument in this matter. We conclude that section 1842 authorizes, and the Fourth Amendment to the Constitution of the United States does not prohibit, an order of the kind described in the FISC's certification. Read fairly and as a whole, the governing statutes evince Congress's understanding that pen registers and trap-and-trace devices will, under some circumstances, inevitably collect content information. Congress has addressed this difficulty by requiring the government to minimize the incidental collection of content through the employment of such technological measures as are reasonably available—not by barring entirely, as a form of prophylaxis, the use of pen registers and trap-and-trace devices simply because they might gather content incidentally.

Nor does an order authorizing such surveillance run afoul of the Fourth Amendment's guarantee against unreasonable searches and seizures. The warrant requirement is generally a tolerable proxy for "reasonableness" when the government is seeking to unearth

Approved for public release by the ODNI 20160818

evidence of criminal wrongdoing, but it fails properly to balance the interests at stake when the government is instead seeking to preserve and protect the nation's security from foreign threat. We therefore hold that surveillance of this type may be constitutionally reasonable even when it is not authorized by a probable-cause warrant. We further hold, on the facts presented here, that the order under review reasonably balances the investigative needs of the government and the privacy interests of the people.

I

On January 21, 2016, a judge of the FISC approved an Application for Pen Register and Trap and Trace Device(s) after finding that the application met the requirements for a pen register/trap-and-trace authorization order under the Foreign Intelligence Surveillance Act ("FISA"). The authorization provided for the installation and use of pen register/trap-and-trace devices on a cellular telephone number used by the subject of an ongoing investigation to protect against clandestine intelligence activities, with the assistance of the service provider for that number.[1]

As requested by the government, the court's order granted "the authority to record and decode all post-cut-through digits," as described in a memorandum filed by the government with the FISC on August 17, 2009, in connection with an earlier request for similar authorization. The court's order further provided that the govern-

[1] A pen register is a device or process that records or decodes dialing signals transmitted from a telephone or other wire or electronic communication instrument or facility. A trap-and-trace device is a device or process that captures incoming signals and therefore identifies the originating number or source of an incoming wire or electronic communication.

Approved for public release by the ODNI 20160818

ment "shall not make any affirmative investigative use of post-cut-through digits acquired through pen register authorization that do not constitute call dialing, routing, addressing or signaling information, unless separately authorized by this Court." In a secondary order, the court directed the service provider to furnish "all information, facilities, or technical assistance necessary to accomplish the installation and operation of the . . . device(s)."

"Post-cut-through digits" are numbers or characters that are dialed after the call is initially connected or "cut through." Frequently, those numbers are other telephone numbers, as when a caller places a calling card, credit card, or collect call by first dialing a carrier access number and then, after the initial call is "cut through," dialing the telephone number of the intended recipient. *See U.S. Telecom Ass'n v. FCC*, 227 F.3d 450, 456, 462 (D.C. Cir. 2000); *In re Application of the United States*, 396 F. Supp. 2d 45, 48 (D. Mass. 2005). Both the first dialed number (the carrier access number) and the second dialed number (the intended recipient's number) constitute dialing information.[2] The initial dialed number, however, is likely to be of little interest to investigators who are seeking to determine what specific number the caller is

[2] The statute that defines pen registers and trap-and-trace devices for the purposes of this case refers to such information as "dialing, routing, addressing, or signaling information" utilized in the processing and transmitting of wire or electronic communications, 18 U.S.C. § 3127(3), (4). That phrase is sometimes represented by the acronym DRAS. For simplicity, we will refer to that information simply as "dialing information," but with the understanding that the term is meant to include all four categories of information set forth in section 18 U.S.C. § 3127, and to exclude what we shall refer to as "content information."

Approved for public release by the ODNI 20160818

calling. In such a situation, in order to discover what number is being called, the investigators must be able to intercept the post-cut-through digits.

In some instances, after a caller has dialed a telephone number, the caller dials additional digits that do not constitute dialing information, but instead constitute a form of content information. For example, after dialing a bank, the caller may be prompted to input a password, a personal identification number, or a bank account number. Or, under certain circumstances, a customer may enter a credit card number or a Social Security number by dialing additional digits. That information is considered content information. As the government acknowledges, pen register orders do not target the interception and decoding of such content information.[3]

The authorization granted by the FISC judge in this case was consistent with prior FISC practice. Since at least 2006, FISC judges have issued pen register/trap-and-trace orders under 50 U.S.C. § 1842 that have authorized the acquisition of all post-cut-through digits, while generally prohibiting the use of those digits that do not constitute dialing information.

[3] The term "contents" has the same meaning in this context as in the federal wiretapping statute, where it is defined to mean "any information concerning the substance, purport, or meaning of [a wire, oral, or electronic] communication." 18 U.S.C. § 2510(8); *id.* § 3127(1). A different definition of "contents" is set forth at 50 U.S.C. § 1801(n). The definitions in section 1801, however, apply to terms "[a]s used in this subchapter"—i.e., in 50 U.S.C. §§ 1801-1812, the FISA subchapter on electronic surveillance. That definition does not apply to "contents" for purposes of the FISA subchapter on pen registers and trap-and-trace devices, 50 U.S.C. §§ 1841-1846.

Approved for public release by the ODNI 20160818

In the order certifying the question of law to this court, the FISC judge set forth in detail the background of the legal issue presented by the government's application. The FISC judge also described the manner in which other courts have dealt with this issue under the pen register/trap-and-trace provisions of title 18 of the United States Code, which govern the use of such devices in the context of criminal investigations.

The FISC judge explained that the pen register/trap-and-trace statutes provide that the information intercepted by pen registers and trap-and-trace devices "shall not include the contents of any communication." 18 U.S.C. § 3127(3), (4). A related section, however, states that the government "shall use technology reasonably available to it" that restricts the recording or decoding of electronic or other impulses "so as not to include the contents of any wire or electronic communications." *Id.* § 3121(c). In the past, the FISC judge explained, the government has argued, and the FISC has accepted, that in the absence of such reasonably available technology, the government is permitted to obtain all post-cut-through digits, so long as the investigative use of any content information contained therein is prohibited. Because there is not now and has not previously been any known or reasonably available technology to segregate dialing information from content information in post-cut-through digits prior to the interception of those digits, the government has contended that it is entitled to obtain post-cut-through digits even when the acquisition of such digits comes with some risk of intercepting content information.

The FISC judge explained that the government's interest in acquiring such digits is concretely presented in this case. The subject of the investigation is suspected of engaging in clandestine intelligence activities on behalf of a foreign government, contrary to the interests of the United States. [redacted]

Approved for public release by the ODNI 20160818

[redacted]

Using currently available technology, the government cannot identify the foreign telephone number without obtaining the entire set of post-cut-through digits.

Considering the competing privacy interests, the FISC judge concluded that they are not great. Even though some post-cut-through digits may constitute content information, they "nonetheless involve a narrow category of information from a subset of calls placed from a targeted phone number." The intrusion, the judge explained, is less than obtaining the full contents of calls to or from a targeted number, and the intrusion is also "mitigated by the prohibition on affirmative investigative use" of the non-dialing information.

In view of the uniformity of the authorities holding that post-cut-through digits may not be intercepted in the parallel setting of criminal investigations, the FISC judge concluded that the "disagreement between the FISC and other courts provides reason to believe that consideration of these issues by the [Foreign Intelligence Surveillance Court of Review] would serve the interests of justice." *See* 50 U.S.C. § 1803(j). We find that it is appropriate for this court to address the certified question.

II

The problem in this case is this: Under presently available technology, there is no way for a pen register to distinguish between dialing information and content information contained in post-cut-through digits so that it can be directed to intercept only the former and not the latter.[4] Therefore, in the case of a pen register order that

[4] The amicus curiae argues that such technology already exists: the government can limit the collection of

Approved for public release by the ODNI 20160818

authorizes the interception of post-cut-through digits, there is some risk that content information will be intercepted along with dialing information. The question we have been asked to decide is whether the statute that authorizes the issuance of pen register orders for foreign intelligence purposes permits courts to authorize the interception of post-cut-through digits, even though there is some risk that such digits might sometimes include content information.

A

The statute that governs the use of pen registers and trap-and-trace devices for foreign intelligence purposes is title IV of FISA, 50 U.S.C. §§ 1841-46. That statute provides that the government can obtain an order authorizing the installation and use of a pen register or trap-and-trace device upon a statutorily sufficient showing, made either to a judge of the FISC or to a properly authorized magistrate judge. *Id.* § 1842.

An application for a pen register or a trap-and-trace device under section 1842 requires the approval of the Attorney General or a designated attorney for the government. *Id.* § 1842(c). It also requires a certification by the applicant 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

---

digits to the first ten dialed digits. To be sure, that approach would exclude all content information, but at the expense of excluding all dialing information that might be present in post-cut-through digits, even in settings where there is no reasonable likelihood of intercepting content information. That is not a technological solution that discriminates between dialing and content information, as referred to in section 3121(c).

Approved for public release by the ODNI 20160818

intelligence activities." *Id.* § 1842(c)(2). Finally, the application must contain a "specific selection term" to be used as the basis for the use of the pen register or the trap-and-trace device. *Id.* § 1842(c)(3). A "specific selection term" is a term "that specifically identifies a person, account, address, or personal device, or any other specific identifier." *Id.* § 1841(4)(A)(i). It must be used to limit, "to the greatest extent reasonably practicable, the scope of information sought, consistent with the purpose for seeking the use of the pen register or trap and trace device." *Id.* § 1841(4)(A)(ii).

Section 1842(h)(1) of FISA provides that the Attorney General "shall ensure that appropriate policies and procedures are in place to safeguard nonpublicly available information concerning United States persons that is collected through the use of a pen register or trap and trace device installed under this section." Section 1842(h)(2) further provides that the FISC is not prohibited from imposing "additional privacy or minimization procedures with regard to the installation or use of a pen register or trap and trace device."

The definitional section of title IV of FISA, section 1841, provides that the terms pen register and trap-and-trace device have the same meanings that are given to those terms in section 3127 of the title 18. The definition of pen register in section 3127 provides as follows, in pertinent part:

> [T]he 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). The definition of "trap and trace device" in title 18 contains similar language:

Approved for public release by the ODNI 20160818

> [T]he term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;

Id. § 3127(4).

B

The question whether title IV of FISA authorizes pen register orders to collect post-cut-through digits turns on the meaning of the definitional language in 18 U.S.C. § 3127(3), and in particular the "proviso" clause, which reads as follows: "provided, however, that such information shall not include the contents of any communication." It is clear that the statutory language is intended to prohibit the use of pen registers for the purpose of intercepting content communications, such as bank account numbers, social security numbers, and personal identification numbers. The statute expresses that intent in an unusual way, however, by making the prohibition against intercepting content information part of the definition of "pen register."[5]

The most literal interpretation of section 3127(3), read in isolation, leads to a problem. If a device ceases to be a pen register whenever it intercepts post-cut-through content information, it is impossible to know in advance

[5] The statutory provisions that apply to trap-and-trace devices are largely (but not entirely) parallel to the provisions that apply to pen registers. Because our analysis of the legal issue presented in this case is the same for both pen registers and trap-and-trace devices, we will generally refer only to pen registers for simplicity.

Approved for public release by the ODNI 20160818

whether the device is a pen register (and thus whether its use may be authorized under title IV of FISA).

A pen register intercepts the digits that are dialed. It does not distinguish between dialing information, on the one hand, and dialed digits that constitute "the contents of any communication," on the other. With currently available technology, that distinction can be drawn only after the information collected by the pen register has been decoded. Defining a device as a pen register depending on the nature of the material it ultimately collects thus poses a dilemma for courts that are asked to authorize the collection of dialing information, and in particular post-cut-through digits. A court seeking to determine whether to authorize a pen register application that includes post-cut-through digits cannot know in advance whether the device will intercept some content information and therefore be ineligible for an authorization order.

One approach to resolving that problem is to conclude that if there is any chance that content information will be intercepted, a pen register order that authorizes the collection of post-cut-through digits may not be entered. Adopting that theory, several courts have held that the pen register statute does not authorize the collection of any post-cut-through digits. *See In re Application of the United States*, 622 F. Supp. 2d 411 (S.D. Tex. 2007); *In re Application of the United States*, No. 6:06-mj-1130 (M.D. Fla. June 20, 2006), *aff'g In re Application of the United States*, No. 6:06-mj-1130 (May 23, 2006); *In re Applications of the United States*, 515 F. Supp. 2d 325 (E.D.N.Y.

Approved for public release by the ODNI 20160818

2007); *In re Application of the United States*, 441 F. Supp. 2d 816 (S.D. Tex. 2006).[6]

The theory adopted by those courts might lead to the conclusion that the collection of post-cut-through digits may be authorized in circumstances in which the govern-

[6] One of the courts that has addressed this issue has concluded that all post-cut-through digits constitute content information. *In re Application of the United States*, No. 08 MC 0595, 2008 WL 5255815 (E.D.N.Y. Dec. 16, 2008). On that premise, the court declined to authorize the interception of post-cut-through digits. That premise, however, is flawed, as it is well understood that post-cut-through digits can include both dialing information and content information, and that they may often include only dialing information.

The amicus curiae argues that all post-cut-through digits are content with respect to the service provider, and that the interception of post-cut-through digits should never be authorized. That argument is unconvincing, as the definition of "contents" for purposes of pen registers is "information concerning the substance, purport, or meaning of [a wire, oral, or electronic] communication." 18 U.S.C. § 2510(8). That definition does not include dialing information, whether viewed from the perspective of the individual or the provider. The fact that the provider is not the one who uses that information for dialing purposes does not alter the fact that the information is dialing information. The FCC made that point in its decision on remand from *U.S. Telecom Ass'n v. FCC*, 227 F.3d 450 (D.C. Cir. 2000), cited by the amicus curiae. The FCC explained that whether particular information is call-identifying information has nothing to do with "whether a carrier uses the dialed digits as part of its own call processing." *In re Communications Assistance for Law Enforcement Act*, 17 F.C.C.R. 6896 (2002).

Approved for public release by the ODNI 20160818

ment can assure the court that it is highly unlikely that content information will be intercepted along with dialing information. None of the above-cited decisions have drawn that distinction, however. Rather, they have flatly barred the government from relying on the pen register statutes to intercept post-cut-through digits. *See In re Application of the United States*, 622 F. Supp. 2d at 422 ("If the Government has no means to exclude collecting content when collecting post-cut-through dialed digits, the Government may not obtain such information under the Pen Register Statute."); *In re Applications of the United States*, 515 F. Supp. 2d at 339 ("Until the Government can separate PCTDD that do not contain content from those that do, pen register authorization is insufficient for the Government to obtain any PCTDD."); *In re Application of the United States*, 441 F. Supp. 2d at 827 ("Post-cut-through dialed digit contents . . . are not available to law enforcement under the Pen/Trap Statute."); *In re Application of the United States*, No. 6:06-mj-1130, at 5 (M.D. Fla. June 20, 2006) ("[T]his Court rejects the United States' argument that it can obtain post-cut-through digits on the lesser showing permitted by the pen register and trap-and-trace statutes.").

We think the better approach is to interpret the definitional language of section 3127(3) to mean that a court may not authorize the use of a pen register to collect content information, and that any content information that is collected cannot be used for any investigative purposes. Under that interpretation, a court can authorize the use of a pen register to collect post-cut-through digits, as long as the collecting agency takes all reasonably available steps to minimize the collection of content information and is prohibited from making use of any content information that may be collected.

We conclude that the latter interpretation of section 3127(3) is more in line with the statutory text and the

Approved for public release by the ODNI 20160818

purpose the provision was intended to serve. In particular, we do not believe Congress intended to prohibit the use of pen registers whenever there was any risk that the intercepted digits would constitute content information. To the contrary, we believe the best interpretation of the related provisions of the pen register statutes is that Congress understood that content information might sometimes be intercepted by authorized pen registers, but intended that steps should be taken to minimize that risk to the extent reasonably possible. Both the text and the legislative history of the pen register statutes support this interpretation of section 3127(3).

1

It is clear from the text of the pen register provisions in title 18, read as a whole, that Congress understood that some content information might be intercepted in the course of executing a valid pen register order. One of those provisions is 18 U.S.C. § 3121(c). The statute states:

> (c) Limitation. A government agency authorized to install and use a pen register or trap and trace device 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, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.

18 U.S.C. § 3121(c).

That language requires the government to use "reasonably available" technology to avoid recording content information. But the prohibition is conditional, requiring the government to use such restricting technology only if it is "reasonably available." Thus, by requiring the use of

Approved for public release by the ODNI 20160818

"technology reasonably available" to restrict recording and decoding of intercepted information to dialing information, Congress recognized that such technology might not be available or might not achieve the objective with perfect accuracy.

The plain import of the statutory language is that, absent such "reasonably available" technology, lawfully authorized pen registers will sometimes intercept and decode content information contained in dialed digits, in addition to information regarding dialing information. Thus, section 3121(c) strikes a compromise that allows the government to obtain the dialing information to which it is entitled, while requiring that all reasonably available measures be taken to avoid or minimize the collection of content information.

As the amicus curiae points out, section 3121(c) is not incorporated by reference in title IV of FISA and therefore does not directly apply to FISA pen register applications. Nonetheless, it is important to our analysis here because it provides guidance in determining how Congress intended courts to interpret the definitional provisions, sections 3127(3) and (4), which apply to both title 18 and title IV of FISA. The argument that section 3121(c) is irrelevant to FISA pen registers also ignores the body of law that teaches that "where words are employed in a statute which had at the time a well-known meaning at common law or in the law of this country they are presumed to have been used in that sense unless the context compels to the contrary." *Lorillard v. Pons*, 434 U.S. 575, 583 (1978) (quoting *Standard Oil v. United States*, 221 U.S. 1, 59 (1911)).

Based on the legislative history of, and amendments to, the criminal pen register statute, and Congress's understanding of the developing technology, it can safely be assumed that Congress—in incorporating the criminal pen register definition into FISA—understood that it was

Approved for public release by the ODNI 20160818

incorporating more than just the definition of a pen register at section 3127. Indeed, the author of what became section 3121(c), Senator Patrick Leahy, was quite clear that the provision was necessary to address the incidental collection of content under a pen register order. 147 Cong. Rec. 20,680 (2001) (statement of Sen. Patrick Leahy). But at the same time Senator Leahy recognized that the government's ability to avoid the collection of content information was subject to the limitations of "reasonably available technology." *Id.*

The amicus curiae takes the position that the definitional language of section 3127(3)—"provided, however, that such information shall not include the contents of any communication"—plainly forecloses the conclusion that a pen register may lawfully intercept content under any circumstances. And some courts, likewise seizing on the "provided" clause of section 3127(3), have dismissed section 3121(c) as a mere "added precaution to ensure that the Government does not use an authorized pen register to collect contents." *In re Application of the United States*, 622 F. Supp. 2d at 421.

We cannot agree with either position. Our duty is "to construe statutes, not isolated provisions," and to properly discharge that duty, "we must read the [statute's] words in their context and with a view to their place in the overall statutory scheme." *King v. Burwell*, 135 S. Ct. 2480, 2489 (2015). Of particular salience here, we are to avoid interpreting one statutory provision in a manner that would render another provision superfluous. *Corley v. United States*, 556 U.S. 303, 314 (2009).

In focusing narrowly on section 3127(3) and giving short shrift to the natural implication of section 3121(c), the amicus curiae's plain-language argument and the "added precaution" theory run afoul of these principles. If section 3127(3) barred courts from authorizing the collection of post-cut-through digits, there would be no need for

Approved for public release by the ODNI 20160818

technology to distinguish between dialing information and content information. The need for technology to distinguish between the two types of information arises only if the courts can authorize investigators to intercept signals that can sometimes contain content. Because only post-cut-through digits can contain content information, the limitation of section 3121(c) must necessarily be directed to post-cut-through digits. And because the limitation in section 3121(c) is conditional, not absolute, the two provisions can be read in harmony only by construing them to permit the interception of post-cut-through digits under appropriate circumstances.[7]

2

The background and development of the provisions of title 18 that authorize the installation and use of pen registers confirm our understanding of the statutory text by shedding further light on the meaning of the pen

[7] The amicus curiae contends that if the government's argument were applied to Internet pen registers, the government could collect information generated by a wide variety of activities on the Internet, including searching, uploading documents, and drafting emails. [redacted] Nonetheless, the amicus argues that the prospect of such collections indicates that the government's statutory construction must be wrong. We disagree. Even assuming that the government's statutory theory would apply in the same manner in that different technological setting, we would have to determine whether any technology is reasonably available to excise content. Moreover, the application of the government's theory in that setting, if it had the consequences argued by amicus curiae, might call for a different Fourth Amendment balancing of interests.

Approved for public release by the ODNI 20160818

register statutes in general, and section 3121(c) in particular.

Prior to 1986, there was no federal statute that governed the use of pen registers and trap-and-trace devices. Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, dealt with the interception of oral or wire communications that could "be overheard and understood by the human ear." S. Rep. No. 99-541, at 2 (1968). Title III was silent, however, as to the use of pen registers or other devices that could intercept non-content information.

In *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court held that the Fourth Amendment does not apply to a pen register that simply monitors the digits dialed on a party's telephone. The Court reasoned that the calling party has voluntarily turned that dialing information over to a third party and has assumed the risk that the third party would turn that information over to the government. Thus, the Court held that pen registers, unlike wiretaps that intercept conversations, could be installed and operated without the need for a court order.

In 1986, Congress changed that regime with the enactment of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848. That statute added a provision authorizing the government to install and use pen registers and trap-and-trace devices, but only upon obtaining a court order. The showing required to obtain such an order was less demanding than the probable cause showing required for a wiretap authorization, however. For the installation and use of a pen register or trap-and-trace device, the statute required only that the government represent that the information being sought was "relevant to an ongoing criminal investigation being conducted" by the requester's agency. 18 U.S.C. § 3122(b) (1988).

Approved for public release by the ODNI 20160818

Eight years later, in the Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279, Congress revisited the use of pen registers and trap-and-trace devices. The legislative history of that statute shows that Congress understood that pen registers were capable of intercepting content information in the course of performing their authorized function of intercepting dialing information.[8] Congress's response to that problem was to direct that the interception of content incidental to the interception of dialing information was to be minimized to the extent that it was technologically feasible to do so.

In particular, Congress added the "limitation" provision, section 3121(c), to the pen register statutes. The enacted version of section 3121(c) stated:

> 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.

18 U.S.C. § 3121(c) (1994).

That provision recognized that pen registers were capable of intercepting content information. Congress's solution to that problem was to direct agencies using pen

---

[8] The problem of pen registers intercepting "content" or "transactional" information was discussed throughout the Joint Hearing on the bill that became the 1994 statute. *See Digital Telephony & Law Enforcement Access to Advanced Telecomms. Techs. and Servs.: Joint Hearings Before the Subcomm. on Tech. and the Law of the S. Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the H. Comm. on the Judiciary*, 103d Cong. 39-40, 50, 110-11, 114, 116, 158, 161 (1994).

Approved for public release by the ODNI 20160818

registers to use technology that was "reasonably available" to restrict the recording or decoding of content information and limit the information obtained to "the dialing and signaling information utilized in call processing." In effect, Congress directed the agencies to do the best they reasonably could to limit the interception of content information, but it did not suggest that, in the absence of such reasonably available technology, a pen register could not be authorized if it posed the risk of intercepting content information.

Both the House and Senate Reports on the 1994 Act explained that the purpose of the amendment was not to prohibit the use of pen registers, but to "require[] law enforcement to use reasonably available technology to minimize information obtained through pen registers." S. Rep. No. 103-402, at 18 (1994); H.R. Rep. No. 103-827, pt. 1, at 17 (1994).[9] In particular, the reports explained that the new provision would require government agencies "to use, when reasonably available, technology that restricts the information captured by such device to the dialing or signaling information necessary to direct or process a call, excluding any further communication conducted through the use of dialed digits that would otherwise be captured." S. Rep. No. 103-402, at 31; H.R. Rep. No. 103-827, pt. 1, at 32.

[9] The term "minimization" has a familiar meaning in the context of interceptions of electronic communications. Section 2518(5) of title 18 directs that electronic surveillance must "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception." The requirement of minimization thus contemplates that some unauthorized interception will inevitably occur, but that the agency must take steps to keep that interception to a minimum.

Approved for public release by the ODNI 20160818

Senator Leahy, the principal sponsor of the legislation, used the same language when explaining the text of the amendment during floor consideration of the legislation in the Senate. *See* 140 Cong. Rec. 20,451 (1994) (statement of Sen. Patrick Leahy).

Accordingly, as matters stood after the 1994 legislation, the government could obtain authorization to use pen registers, even though those devices might in some instances intercept content information, as long as the government used all technology that was reasonably available to minimize the extent to which such content information was intercepted and decoded.

Four years later, Congress amended FISA by adding the pen register and trap-and-trace provisions of title IV, 50 U.S.C. § 1841 et seq. The new section 1841 provided that the terms "pen register" and "trap and trace device" were to "have the meanings given such terms in section 3127 of title 18." Pub. L. No. 105-272, 112 Stat. 2396, § 601 (1998).

Following the attacks against New York and Washington on September 11, 2001, Congress enacted the USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272. Among many other provisions, Congress modified portions of the pen register/trap-and-trace statute. The changes made at that time are at the heart of the issue before the court today.

The principal change to the pen register/trap-and-trace provisions was to make those provisions applicable not just to telephony, but to all forms of wire and electronic communications. In so doing, Congress made four amendments that bear on the present issue.

First, Congress omitted the words "call processing" and added the words "routing" and "addressing" to section 3121(c) to cover technologies other than telephony. *Id.* § 216(a).

Approved for public release by the ODNI 20160818

Second, Congress modified section 3121(c) to state explicitly that the purpose of directing the government to use "reasonably available" technology to limit the collection of certain electronic signals was "so as not to include the contents of any wire or electronic communications." *Id.*

Third, Congress amended the definition of "pen register" by expanding the definition to include "dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." *Id.* § 216(c).

Fourth, Congress added the proviso in the definitions of pen register and trap-and-trace device that read: "provided, however, that such information shall not include the contents of any communication." *Id.*

The USA PATRIOT Act was enacted seven weeks after the September 11, 2001, attacks, and in light of the speed with which it was enacted, there is only limited legislative history for the statute. The changes to sections 3121(c) and 3127 were added in the Senate. In the absence of a committee report, Senator Leahy, the chairman of the Senate Judiciary Committee, presented a detailed summary of the changes on the day before the Act was passed. He explained that the language used in the pen register and trap-and-trace statutes was intended "to expressly exclude the use of pen-trap devices to intercept 'content' which is broadly defined in 18 U.S.C. 2510(8)." 147 Cong. Rec. 20,680 (2001) (statement of Sen. Patrick Leahy). He added that the Act "requires the government to use reasonably available technology that limits the interceptions under the pen/trap device laws 'so as not to include the contents of any wire or electronic communications.'" *Id.*

Importantly, Senator Leahy recognized that, notwithstanding the statutory directive to use reasonably available technology to avoid collecting content information, the

Approved for public release by the ODNI 20160818

"pen/trap devices in use today collect 'content.'" *Id.* In particular, he recognized the risk of collecting content information from "[t]he impulses made after a phone call is connected." *Id.* He explained that the amendment to section 3121(c) was intended to underscore the need to incentivize the development of better technology to limit the interception of content information, particularly in light of the fact that the USA PATRIOT Act made the pen register provisions applicable to a wide array of modern communications technologies, such as the Internet, and not simply traditional telephone lines. *See also* H.R. Rep. No. 107-236(I), at 52-53 (2001).

Senator Leahy stated that he was concerned that in broadening the types of dialing information that could be intercepted to include routing and addressing information, Congress might be misunderstood as authorizing the interception of content information. He said that to address that issue, he had favored including definitions of those terms in the 2001 statute, but that the administration had objected. Instead, to address his concerns, the administration agreed to include the references to content information in sections 3121(c) and 3127(3) and (4).

Senator Leahy also noted that, in light of the known risk of collecting content information from post-cut-through digits, he would have preferred a requirement of somewhat heightened judicial review for pen register and trap-and-trace applications. But in the absence of such a requirement, he acknowledged that the statute continued to require only that the government "use reasonably available technology" to limit the collection of content information.

Senator Leahy's comments make clear that the new language added in the 2001 statute was intended to avoid expanding the type of information that could be intercepted, not to narrow it. In particular, nothing in his comments, or elsewhere in the legislative history, suggests

Approved for public release by the ODNI 20160818

that, in the absence of an effective technological solution, the amendments to the pen register/trap-and-trace statutes were intended to prohibit the collection of dialing information simply because there was some risk that content information might incidentally be collected as well.

Analysis of the sequence of pertinent statutes leads us to conclude that Congress recognized, from as early as 1994, that judicial authorization to collect post-cut-through digits posed the risk that some content information would be intercepted. But Congress chose to deal with that risk by requiring the government to use reasonably available technology to minimize the extent to which such content information was collected. It could have dealt with that risk by preventing the collection of post-cut-through digits altogether, but it did not.

We therefore conclude that a close analysis of the statutes that have authorized pen register orders starting in 1986 does not support the view that Congress sought to prohibit any authorized collection of dialing information whenever it posed some risk of additionally collecting content information. What Congress elected was a course of minimization, principally through the use of "reasonably available technology."

III

Our analysis of the pen register statutes requires us to consider whether those statutes, if construed to authorize the interception of post-cut-through digits, would run afoul of the Fourth Amendment.

As noted above, the Supreme Court in *Smith v. Maryland* held that the use of a pen register to collect the numbers dialed on a target telephone does not constitute a "search" for Fourth Amendment purposes. The *Smith* case, however, involved the use of a pen register to obtain dialing information only; no content information was at

Approved for public release by the ODNI 20160818

issue in that case, in the form of post-cut-through digits or otherwise.

It may be that if a pen register interception were directed at the acquisition and use of content information, it would be unlawful in the absence of a court order issued on a showing of probable cause. In the context of criminal investigations, that would certainly be the case for the interception of conversations through electronic surveillance, *Berger v. New York*, 388 U.S. 41 (1967), and it has been held that probable cause is required to authorize the disclosure and use of content information in email communications, *see Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007), *vacated*, 532 F.3d 521 (6th Cir. 2008) (en banc). The same rule might apply to the use of a pen register for the purpose of intercepting content information.

But the FISC judge's authorization order for post-cut-through digits does not target content information; it targets dialing information. If content information is collected at all, the collection of that information is incidental, and the FISC judge's authorization order directs that no investigative use be made of that information (at least in the absence of a further order from the court). The constitutional issue, therefore, is not whether a probable cause warrant is required to use a pen register to obtain content information for investigative purposes. Rather, the question is whether the risk of incidental collection of content information renders the collection of dialing information in post-cut-through digits unreasonable in the absence of a probable cause warrant, even when the content information will not be used for any purpose. We think the answer to that question is no.

The touchstone of the Fourth Amendment is reasonableness. *Riley v. California*, 134 S. Ct. 2473, 2482 (2014); *United States v. Knights*, 534 U.S. 112, 118 (2001); *see also Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 652

Approved for public release by the ODNI 20160818

(1995); *In re Sealed Case*, 310 F.3d 717, 742 (F.I.S.C.R. 2002). In determining the reasonableness of particular governmental action, the court must assess, "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 legitimate governmental interests." *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999); *see also Tennessee v. Garner*, 471 U.S. 1, 8 (1985); *United States v. Place*, 462 U.S. 696, 703 (1983); *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1012 (F.I.S.C.R. 2008).

When law enforcement officials undertake a search to uncover evidence of criminal wrongdoing, the familiar requirement of a probable-cause warrant generally achieves an acceptable balance between the investigative needs of the government and the privacy interests of the people. *See Vernonia Sch. Dist. 47J*, 515 U.S. at 653. But it has long been recognized that some searches occur in the service of "special needs, beyond the normal need for law enforcement," and that, when it comes to intrusions of this kind, the warrant requirement is sometimes a poor proxy for the textual command of reasonableness. *Id.*

We conclude that, in the circumstances presented here, the incidental collection of content information during the collection of post-cut-through digits—assuming it constitutes a search in the first place—is constitutionally reasonable, even when done without a probable-cause warrant.

The idea that official intrusions calculated to preserve the nation's security against foreign threat might require special constitutional treatment is not a new one. In *Katz v. United States*, the first page in the modern chapter of our search-and-seizure jurisprudence, the Supreme Court paused to observe that the Fourth Amendment's usual strictures might require adjustment "in a situation involving national security." 389 U.S. 347, 358 n.23 (1967).

Approved for public release by the ODNI 20160818

Five years later, in *United States v. United States District Court (Keith)*, the Court rejected the argument that no warrant need be obtained whenever the government engages in domestic surveillance related to "internal security matters." 407 U.S. 297, 299 (1972). But it took care to emphasize that *Keith* "involve[d] only the domestic aspects of national security," not any "issues which may be involved with respect to activities of foreign powers or their agents," *id.* at 321-22, and it noted "the view that warrantless surveillance, though impermissible in domestic security cases, may be constitutional where foreign powers are involved," *id.* at 322 n.20.

Consistent with this counsel, in the decade following *Keith*, a number of federal appeals courts recognized a "foreign intelligence" exception to the warrant requirement. *See United States v. Truong Dinh Hung*, 629 F.2d 908, 912-16 (4th Cir. 1980); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977); *United States v. Butenko*, 494 F.2d 593, 604-06 (3d Cir. 1974) (en banc); *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973). *But see Zweibon v. Mitchell*, 516 F.2d 594, 633-51 (D.C. Cir. 1975) (en banc) (plurality opinion) (suggesting, in dictum, that no such exception exists).[10]

---

[10] The dictum in *Zweibon* was not joined by a majority of the court. As the D.C. Circuit has recognized in subsequent cases, the *Zweibon* court barred "warrantless electronic surveillance of persons not suspected of collaboration with foreign interests adverse to this country," but "there was no opinion of the court on the question of warrantless electronic surveillance of collaborators or suspected collaborators of foreign interests." *Halperin v. Helms*, 690 F.2d 977, 1000 n.82 (D.C. Cir. 1982); *see also Ellsberg v. Mitchell*, 709 F.2d 31, 66 n.63 (D.C. Cir. 1983); *United States v. Belfield*, 692 F.2d 141, 145 (D.C. Cir.

Approved for public release by the ODNI 20160818

Truong is illustrative. In that case, the FBI became aware that David Truong, a Vietnamese citizen living in the United States, was obtaining classified papers from a source within the federal government and endeavoring to send them to Vietnamese officials in Paris. 629 F.2d at 911-12. With the approval of the Attorney General, but no judicial warrant, Truong's phone was tapped and his apartment "bugged." *Id.* at 912. He challenged the admission at trial of evidence obtained through this warrantless surveillance, but the district court admitted much of it, and the Fourth Circuit affirmed. The appeals court observed that, in the area of foreign intelligence, the needs of the executive are particularly "compelling," and that a warrant requirement would cripple the government's ability to counter threats from abroad with the needed "stealth, speed, and secrecy." *Id.* at 913. Accordingly, it held that a search may be constitutionally reasonable, notwithstanding the absence of prior judicial authorization, when "the object of the search or the surveillance is a foreign power, its agent or its collaborators," and "the search is conducted *primarily for foreign intelligence reasons*." *Id.* at 915 (emphasis supplied) (internal quotation marks omitted).[11]

More recently, this court both acknowledged the existence of a foreign-intelligence exception to the warrant requirement and explained its doctrinal underpinnings. *See In re Directives*, 551 F.3d at 1010-12. In *In re Directives*, we noted that in so-called "special needs" cases, the Supreme Court has "excused compliance with the War-

---

1983); *Chagnon v. Bell*, 642 F.2d 1248, 1259 (D.C. Cir. 1980).

[11] Consistent with this "primary purpose" requirement, the court affirmed the exclusion of evidence gleaned after the date when the government had "begun to assemble a criminal prosecution." *Truong*, F.2d at 916.

Approved for public release by the ODNI 20160818

rant Clause when the purpose behind the government action went beyond routine law enforcement and insisting upon a warrant would materially interfere with the accomplishment of that purpose." *Id.* at 1010. The government may, for instance, engage in certain warrantless intrusions when it acts as educator; blind adherence to the Warrant Clause in the public schools "would unduly interfere with the maintenance of the swift and informal disciplinary procedures that are needed, and . . . undercut the substantial need of teachers and administrators for freedom to maintain order." *Vernonia Sch. Dist. 47J*, 515 U.S. at 653. So too may it maintain sobriety checkpoints at which vehicles are stopped (and drivers thereby seized) without suspicion, in the interest of curbing the harms occasioned by drunk driving. *Michigan Dep't of State Police v. Sitz*, 496 U.S. 444, 450-51 (1990).

We recognized in *In re Directives* that when the government engages in foreign intelligence surveillance—no less than when it acts to maintain discipline in the schools or operates sobriety checkpoints—its needs go beyond "any garden-variety law enforcement objective," and its objectives would be seriously hampered by the requirement of a warrant. *In re Directives*, 551 F.3d at 1011. Collecting foreign intelligence with an eye toward safeguarding the nation's security serves an interest—a "particularly intense" interest—different from the government's interest in the workaday enforcement of the criminal law.[12] And if the government were constrained

[12] In discussing the importance of the government's interest in preserving and protecting national security, we criticized *Truong*'s primary-purpose requirement as "unstable, unrealistic and confusing." *In re Directives*, 551 F.3d at 1011 (internal quotation marks omitted). "A surveillance with a foreign intelligence purpose," we observed, "often will have some ancillary criminal-law

Approved for public release by the ODNI 20160818

to obtain a warrant before undertaking any foreign intelligence gathering that constituted a search, its "ability to collect time-sensitive information" would be "hinder[ed]" and "the vital national security interests at stake" impeded. *Id.* We thus held that the Fourth Amendment does not require a probable-cause warrant "when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States." *Id.* at 1012.

In re Directives virtually controls this case. The relevant statute at issue in this case authorizes the use of a pen register "to obtain foreign intelligence information . . . to protect against . . . clandestine intelligence activities." 50 U.S.C. § 1842(a)(1). Pursuant to that statute, the government seeks to monitor the dealings of a person, currently in the United States, who is suspected of collecting intelligence in the service of a foreign power. The purpose of the proposed monitoring is the preservation of national security. Few government interests are of a higher order. The interest at stake is no less—and may even be greater—for the foreign agent's being present in this country. And were we to insist on a showing of probable cause and the issuance of a judicial warrant in this setting, we would impede the Executive's ability to bring to bear against the threat those faculties—"stealth, speed, and secrecy," *Truong*, 629 F.2d at 913—needed to secure the nation's well-being in this most fundamental and sensitive of government endeavors.

We thus conclude that when the government, acting pursuant to a program of surveillance involving a legiti-

---

purpose." *Id.* We therefore concluded that the more sensible requirement was that the "programmatic purpose" of the intelligence-gathering "involve[] some legitimate objective beyond ordinary crime control." *Id.*

Approved for public release by the ODNI 20160818

mate objective that goes beyond everyday crime control, seeks to use a pen register directed at a person located in the United States who is reasonably believed to be engaged in clandestine intelligence activities on behalf of a foreign government, it may do so without obtaining a probable-cause warrant even if its monitoring of post-cut-through digits constitutes a search under the Fourth Amendment.

This is not to say, of course, that the Fourth Amendment has no role to play in such cases. It is only to say that, in this context, the warrant requirement is ill-suited to gauge what is reasonable. The textual command of reasonableness—"the ultimate touchstone of the Fourth Amendment," *Riley*, 134 S. Ct. at 2482—still governs. Indeed, it retains its whole force.

We now turn to the question of reasonableness, a question that requires us to balance against the degree of the government's intrusion on individual privacy the degree to which that intrusion furthers the government's legitimate interests. *Houghton*, 526 U.S. at 300. In the circumstances presented here, the scale tips in the government's favor. The search, assuming it is one, is reasonable. In particular, the factors that render the search reasonable are (1) the paramount interest in investigating possible threats to national security; (2) the investigative importance of having access to the dialing information provided by post-cut-through digits, (3) the incidental nature of the collection of content information from post-cut-through digits, (4) the relatively slight intrusion on privacy entailed by the acquisition of post-cut-through digits, (5) the prohibition against the use of any content information obtained from the pen register or trap-and-trace device, (6) the steps taken by the government to minimize the dissemination of post-cut-through digits; and (7) the fact that FISA pen register interceptions are conducted only with the approval and under the supervi-

Approved for public release by the ODNI 20160818

sion of a neutral magistrate, in this case a FISC judge. We discuss each of those factors in more detail below.

First, the Supreme Court has stated that "no governmental interest is more compelling" than national security. *Haig v. Agee*, 453 U.S. 280, 307 (1981); *see In re Directives*, 551 F.3d at 1012 (the governmental interest in national security "is of the highest order of magnitude"); *In re Terrorist Bombings of U.S. Embassies*, 552 F.3d 157, 174 (2d Cir. 2008). Thus, the government's investigative interest in cases arising under FISA is at the highest level and weighs heavily in the constitutional balancing process.

Second, as the facts of this case demonstrate, the dialing information in post-cut-through digits may be of critical investigative importance in certain cases in which pen register authorization is sought. If the subject of a pen register uses a calling service, a pen register that does not collect post-cut-through digits will disclose no information at all about the ultimate destination of the call. Because subjects of national security investigations seek to avoid detection of their activities, the loss of access to post-cut-through digits is likely to substantially undercut the value of a pen register in a significant number of cases.

Third, a pen register authorized in a FISA investigation is targeted at dialing information; the collection of any content information from post-cut-through digits is incidental to the purpose of the pen register. The incidental collection of constitutionally protected material does not render the authorized collection of unprotected material unlawful. *See In re Directives*, 551 F.3d at 1015 (citing *United States v. Kahn*, 415 U.S. 143 (1974), and *United States v. Schwartz*, 535 F.2d 160 (2d Cir. 1976) ("Incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful.")).

Approved for public release by the ODNI 20160818

The application of that rule to searches of documents is particularly instructive here. The Supreme Court recognized in *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976), that "[i]n searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized." The incidental examination of such documents to determine whether they are subject to authorized seizure is analogous to the examination of post-cut-through digits to determine if they contain content information; once it is determined that particular post-cut-through digits contain content information, that information is excluded from any investigative use.

Fourth, the content information found in some post-cut-through digits is likely to be of marginal privacy value. As the FISC judge explained in the certification order, post-cut-through digits that constitute contents "involve a narrow category of information from a subset of calls placed from a targeted phone number" and thus represent "a lesser intrusion than, for example, obtaining the full contents of all calls to or from a targeted phone number." For that reason, in balancing the seriousness of the invasion of the individual's personal privacy against the importance of the government's interest, the degree of the intrusion resulting from collecting post-cut-through digits will typically be modest.

Fifth, as the FISC judge's authorization order makes clear (and is uniformly reflected in FISC pen register/trap-and-trace authorization orders), any content information that is collected as part of the interception of post-cut-through digits may not be used for any investigative purpose, absent an order from the court.[13] That

[13] The government advises us that in the course of its pen register investigations, no such order has ever been

Approved for public release by the ODNI 20160818

prohibition on use protects against the risk that an investigative agency might seek to obtain authorization to intercept post-cut-through digits in order to obtain access to the content information contained therein.

Sixth, minimization procedures are available, and are regularly employed, to limit the extent to which content information that is incidentally intercepted during the collection of post-cut-through digits is made available to, or used and disseminated by, government agents.

The Department of Justice has taken several steps to minimize access to post-cut-through digits and reduce the risk that content information will be intercepted or disclosed. The prohibition against targeting or using content information obtained from post-cut-through digits was set forth in a 2002 memorandum of the Deputy Attorney General, and the FBI's field offices have been instructed to implement procedures to ensure compliance with the policies in that memorandum. *See* Memorandum from Larry D. Thompson, Deputy U.S. Attorney Gen., Avoiding Collection and Investigative Use of "Content" in the Operation of Pen Registers and Trap and Trace Devices (May 24, 2002).

Among those procedures is a measure that requires masking post-cut-through digits in investigative file materials. Only an analyst who has undergone special training may unmask the post-cut-through digits, and only after providing justification for doing so. Record on Appeal, Tab 3, at 17-20. In some circumstances, depending on the nature of the subscriber to the telephone that was initially contacted, even an analyst may not examine post-cut-through digits. For example, if the initial con-

---

granted; in fact, the government has never even sought such an order. *See also* Record on Appeal, Certification at 2 n.1.

Approved for public release by the ODNI 20160818

nection is to a financial institution, an analyst may not examine any post-cut-through digits because there is reason to believe that post-cut-through digits may contain content.

Minimization measures have been recognized as important to the lawfulness of investigative procedures in various settings. Most significantly, federal wiretap law recognizes that some conversations that were not intended to be intercepted will inevitably be overheard. The answer given by Congress and endorsed by the courts is to require minimization of such intrusions to the extent reasonably practicable. *See Scott v. United States*, 436 U.S. 128, 139-43 (1978); *Drimal v. Tai*, 786 F.3d 219, 223-24 (2d Cir. 2015); *United States v. Glover*, 681 F.3d 411, 420-21 (D.C. Cir. 2012).

The Supreme Court has applied the same principle to document searches, emphasizing the importance of minimization in both settings. *See Andresen*, 427 U.S. at 482 n.11 ("In both kinds of searches [searches of conversations and searches of documents], responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy."). And in other Fourth Amendment contexts as well, the Supreme Court has emphasized the importance of minimization steps employed to reduce the intrusiveness of the invasion in question. *See, e.g., Maryland v. King*, 133 S. Ct. 1958, 1979-80 (2013) (acquisition of arrestees' DNA less intrusive because authorized for use only for limited purpose of identification); *Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cty. v. Earls*, 536 U.S. 822, 832-33 (2002) (school drug testing program less intrusive because results kept in confidential files and used for only limited purposes); *Vernonia School Dist. 47J*, 515 U.S. at 658 (school drug testing program less intrusive because of limited purpose of tests and limited dissemination of results).

Approved for public release by the ODNI 20160818

Finally, an important aspect of the use of pen registers in FISA investigations is the role played by FISC judges in authorizing and supervising pen register interceptions. Although the court does not require a showing of probable cause to authorize pen register interceptions, it is responsible for supervising the execution of pen register orders. As noted above, title IV of FISA contains a provision authorizing FISC judges "to impose additional privacy or minimization procedures with regard to the installation or use of a pen register or trap and trace device." 50 U.S.C. § 1842(h)(2).

In appropriate circumstances, FISC judges can use that authority to ensure that the interception of content information through the collection of post-cut-through digits is kept to a minimum, consistent with the government's right to intercept dialing information. Besides requiring that the government use all reasonably available technology to minimize or eliminate the collection of content information, FISC judges can insist that the government assess the risk of intercepting content information in particular cases and can deny authorization for post-cut-through digits (or impose further restrictions) when that risk is deemed to be unacceptably high as, for example, in the case of a request to renew an application for a pen register that has previously intercepted a substantial amount of content information.[14]

The judicial scrutiny of pen register applications and the supervision of the execution of pen register orders further reduces the risk that such measures will be em-

[14] In addition to the statutory authorization for the imposition of minimization procedures, FISA contains a suppression remedy that is available if information from pen registers or trap-and-trace devices was unlawfully acquired or if the devices were not operated in conformity with the authorizing order. 50 U.S.C. § 1845(e)(1).

Approved for public release by the ODNI 20160818

ployed under circumstances, or in a manner, that unreasonably intrudes on individuals' privacy interests.

In sum, we hold that the request in this case for authorization to intercept post-cut-through digits satisfies the reasonableness standard of the Fourth Amendment. Put another way, the Constitution does not go so far as to impose an across-the-board prohibition on the collection of dialing information in the absence of probable cause, simply because of the risk that some content information will be incidentally intercepted as well.

IV

We conclude that Congress intended to minimize the collection of content information by insisting that reasonably available technology be used to segregate dialing information from content information. The government represents--and we have no reason to doubt—that no such technology is currently reasonably available. In that circumstance, we conclude that the government is not barred from using pen registers and trap-and-trace devices to intercept post-cut-through digits because of the risk that the use of those devices might, in some instances, intercept digits that turn out to constitute content information.

It is true that Congress intended to bar courts from authorizing the use of pen registers that target content information. That is not to say, however, that Congress intended to prevent the use of pen registers for the legitimate purpose of obtaining dialing information simply because there was some risk that the pen registers would inadvertently intercept content information in the course of an authorized and lawful interception.

For the reasons set forth above, we answer the certified question in this matter as follows: the FISC may authorize the collection and decoding of post-cut-through digits as long as the government is prohibited from mak-

Approved for public release by the ODNI 20160818

ing investigative or evidentiary use of any content information contained in that material, and as long as the court directs that appropriate procedures be used to minimize the collection of content information, including the use of any reasonably available technology that may be developed to restrict the recording and decoding of pen register or trap-and-trace information to dialing information.