APPROVED FOR PUBLIC RELEASE

CLASSIFIED BY: NSICG [redacted]
REASON: 1.4 (C)
DECLASSIFY ON: 12-31-20 b6 Per FBI
DATE: 01-12-2022 b7C

United States Foreign Intelligence
Surveillance Court of Review

MAR 28 2016

Clerk of Court

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

SURVEILLANCE COURT OF REVIEW

FOREIGN INTELLIGENCE

[redacted] (S)

b1 Per FBI
b3
b7E

SOMMER

Suite 250

20036

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENT OF THE CASE

A. Introduction

The question presented is straightforward: where the government cannot collect the post cut-through dialed digits ("PCTDD") that are used for routing purposes (such as telephone numbers that are dialed after a call is connected) without also collecting the PCTDD that contain the contents of communications (such as financial account numbers), may the government collect all the digits and sort them out later? Every court to consider the issue other than the FISC has answered no. And not just no, but clearly no. The intellectual gymnastics the government employs to reach a contrary conclusion are not persuasive because the government's view does not comport with the plain language of the relevant statutes and conflicts with Congressional intent. Not only is the commandment against collecting contents expressly set forth in the definitions of "pen register" and "trap and trace device," but FISA does not incorporate the key "Limitation" provision that the government misreads as support for its position.

In the criminal context, the federal judiciary is in agreement. Although in national security cases, the Government may have more flexibility to utilize reasonable post-collection safeguards to satisfy the Fourth Amendment, the fundamental limiting factor here is statutory. Congress never authorized the use of pen registers and trap and trace devices to engage in the potential collection of any

contents of communications—whether incidental or targeted—followed by post-collection minimization. Instead, because pen registers and trap and trace orders must only meet a minimal relevance standard,[1] Congress expressly prohibited collecting communication contents.

In 1994, and again in 2001, after learning that law enforcement was improperly collecting content using pen registers despite express prohibitions on doing so, Congress supplemented the statutory definitions with a requirement (not a request) that the government deploy technology to implement the statutory prohibition. The result is that where content and non-content cannot be sorted, the government must use a higher standard of process to collect such mixed communications. Accordingly, as a statutory matter, the government cannot collect PCTDD in the first instance, regardless of what subsequent safeguards the government uses to prevent the subsequent use of the improperly collected information. The solution to the government's problem lies either with the development of better technology or with Congress, not the courts.

B. Procedural Posture

This Court certified a novel question of law under 50 U.S.C. § 1803(j) to address whether the FISC's unique practice of allowing the collection of PCTDD

[1] See In re Application of the United States, 846 F. Supp. 1555, 1558-59 (M.D. Fla. 1994) (noting that in the criminal context a court must accept a certification on its face); United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995) (the judicial role for PR/TTs is "ministerial in nature.").

pursuant to a pen register order is permissible. On February 17, 2016, this Court appointed the undersigned to serve as *Amicus Curiae* for purposes of assisting the Court in considering whether it should affirm the FISC's ruling allowing the Government to collect PCTDD pursuant to its pen register authority. (Order Appointing an *Amicus Curiae* and Briefing Order, Feb. 17, 2016).

As the Court recognized, the certified question arises from a practice that is unique in the FISC. The FISC is the only court to seriously consider the issue that has allowed the government to use pen register and trap and trace authority to collect PCTDD. Every other court that has written about the issue has rejected such requests.[2] Those Courts have refused to read 18 U.S.C. § 3121(c) as broadly as the Government or the FISC, and have precluded the Government from obtaining all PCTDDs in the absence of reasonably available technology to sort content from non-content in advance of collection. Although those opinions are

[2] In re Application of the United States, 441 F. Supp. 2d 816 (S.D. Tex. 2006) ("Smith"); In re Application of the United States, 622 F. Supp. 2d 411 (S.D. Tex. 2007) ("Rosenthal"); In re Application of the United States, 632 F. Supp. 2d 202 (E.D.N.Y. 2008) ("Garaufis"); In re Application of the United States, No. 08-0MC-0595, 2008 WL 5255815 (E.D.N.Y. Dec. 16, 2008) ("Orenstein"); In re Applications of the United States, 515 F. Supp. 2d 325 (E.D.N.Y. 2007) ("Azarack") aff'd Nos. 06-mc-547, 06-mc-561, 07-mc-120, 07-mc-400 (E.D.N.Y. 2007); In re Application of the United States, No. 6:06-mj-1130 (M.D. Fla. May 23, 2006) ("Spaulding") aff'd No. 6:06-mj-1130 (M.D. Fla. June 20, 2006) ("Conway"). Because the names of these cases are substantially similar, the brief references these cases by the name of Magistrate or Judge who wrote the opinions.

not binding here, *Amicus* believes the reasoning of these courts is correct, and the prior practice of the FISC should be reversed.

C. Statutory Background

The Government's authority to obtain pen registers is part of an extensive statutory scheme that occupies the field of government surveillance and includes the Wiretap Act, 18 U.S.C. § 2510, *et seq.*, the Stored Communications Act ("SCA"), 18 U.S.C. § 2701, *et seq.*, the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1801 *et seq.* and the Pen Register Statute, 18 U.S.C. § 3121. Each act serves separate purposes. The Wiretap Act governs the interception and collection of communications in transit. The SCA governs the production of stored communications and customer information from providers. The PR/TT statute governs the real-time collection of non-content information that service providers use to route communications. And FISA implements all three types of surveillance and collection for foreign intelligence investigations.

Congress added the pen register statute in 1986 as part of the Electronic Communications Privacy Act ("ECPA"), Pub. L. 99-508, 100 Stat 1848 (1986), § 301. ECPA expanded the Wiretap Act by amending it to cover electronic communications, to address access to stored communications and customer information, and to fill a void and define when the government can collect non-content information used to route communications in real time. ECPA §§ 101,

301. ECPA altered the definition of "contents" under the 18 U.S.C. § 2510(8), by eliminating information related to the "identity of the parties to such communications or the existence." ECPA, § 101(a)(5). Doing so made the Wiretap Act consistent with Smith v. Maryland, 442 U.S. 735 (1979), which held that monitoring numbers dialed to route a call was not a search under the Fourth Amendment, and did not require a probable cause finding. Congress also added chapter 206 to title 18, which created a statutory scheme for law enforcement's use of pen registers. ECPA, § 301. ECPA initially defined a pen register as

> a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer or a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

ECPA, § 301. Similarly, ECPA defined a trap and trace device as "a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted." Id.

When it passed ECPA, Congress believed that pen registers, by definition and function, could not intercept content:

> The term 'pen register' means a device which records or decodes electronic or other impulses which identify the numbers dialed or

> otherwise transmitted for the purpose of routing telephone calls, with respect to wire communications, on the phone line to which such device is attached. The term does not include the contents of a communication, rather it records the numbers dialed."

H.R. Rep. No. 99-647, at 78 (1986) (emphasis added); S. Rep. 99-541 at *10 (Pen registers "capture no part of an actual telephone conversation, but merely the electronic switching signals that connect two telephones.")[3]

Later, in 1994, Congress enacted the Communications Assistance for Law Enforcement Act ("CALEA"), Pub. L. 103-414, 108 Stat. 4279 (1994), which along with requiring certain providers to alter their systems to allow for real-time surveillance, addressed the issue that law enforcement may be able to collect some content information using a pen register. As the Senate Report on the bill states, Congress intended to ensure that "Call identifying information obtained pursuant to pen register and trap and trace orders may not include information disclosing the physical location of the subscriber sending or receiving the message, except to the extent that location is indicated by the phone number." S. Rep. 103-402 (1994). Likewise, FBI Director Freeh stated he did not want pen registers to allow for the collection of content—much of which would have been collected as PCTDD:

> SENATOR LEAHY: You say this would not expand law enforcement's authority to collect data on people, and yet if you're going to the new technologies, where you can dial up everything from

[3] Because of the technology limitations on traditional pen registers, courts have referred to the limitations on them as "self-regulatory." See People v. Bialostok, 610 NE.2d 374 (NY 1993).

> a video movie to do your banking on it, you are going to have access to a lot more data, just because that's what's being used for doing it.
>
> DIRECTOR FREEH: I don't want that access, and I'm willing to concede that. What I want with respect to pen registers is the dialing information, telephone numbers which are being called, which I have now under pen register authority. As to the banking accounts and what movie somebody is ordering in Blockbuster, I don't want it, don't need it, and **I'm willing to have technological blocks with respect to that information**, which I can get with subpoenas or other processes. I don't want that in terms of my access, and that's not the transactional data I need.

Wiretapping: Joint Hearing of the Technology and Law Subcomm. Of the Senate Judiciary Comm. And the Civil and Constitutional Rights Subcomm. of the House Judiciary Comm., 103d Cong., 2d Sess. 50 (March 18, 1994).

To address this issue, Congress added an additional limitation on law enforcement's use of pen registers in 18 U.S.C. § 3121(c), which provided that:

> "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. This language can be fairly understood to have been inserted precisely to stop the collection of any PCTDD. According to Senator Leahy, "When I added the direction to use reasonably available technology (codified as 18 U.S.C. § 3121(c)) to the pen register statute as part of the Communications Assistance for Law Enforcement (CALEA) in 1994, I recognized that these devices collected content and that such collection was unconstitutional on the mere

relevance standard." 147 Cong. Rec. S10990, S10999 (Oct. 25, 2001). Importantly, the mandate was added to the law when the technology required to be used was intended to restrict the collection to call processing data and thus collection of any PCTDD not used for that purpose was to be precluded. Thus the technology mandate cannot be viewed as license to collect any forms of PCTDD.

In 1998, Congress added a pen register provision to FISA to authorize and regulate the use of pen registers for foreign intelligence purposes. Intel. Auth. Act for Fiscal Year 1999, Pub. L. 105-272, 115 Stat. 2396 (1998). Congress adopted the same definitions of pen registers and trap and trace devices as in the criminal pen register statute, but did not incorporate § 3121(c). Pub. L. 105-272, § 601.

In the USA PATRIOT ACT of 2001, Pub. L. 107-56, 115 Stat. 272 (2001), Congress expanded the use of pen registers outside the context of information used only to route telephone calls, allowing the use of pen register and trap and trace devices on the Internet. See Orin Kerr, Internet Surveillance Law After the USA PATRIOT Act: The Big Brother that Isn't, 97 N.W.U. L. Rev. 607, 637 (Winter 2003).

To remove any doubt that the change in definition could allow collection of communication contents, Congress made three changes simultaneously. First, Congress amended the definition of pen registers as follows (with deletions struck through and additions underlined):

> "a device or process which records or decodes ~~electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached~~ 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, but such term does not include any device or process used by a provider or customer of a wire communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer or a wire communication service for cost accounting or other like purposes in the ordinary course of its business;"

USA PATRIOT Act, § 216. Second, Congress made parallel changes to the definition of "trap and trace device" as follows:

> "a device or process which captures the incoming electronic or other impulses which identify the originating number ~~of an instrument or device from which a wire or electronic communication was transmitted~~ 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...."

Third, Congress amended § 3121(c) as follows,

> 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 and signaling information utilized in ~~call processing~~ the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications. Id.

As Senator Leahy explained, he added this provision, notwithstanding the fact

that he had already inserted the technology mandate in 1994 because

> Nevertheless, the FBI advised me in June 2000 that the pen register devices for telephone services 'continue to operate as they have for decades' and that 'there has been no change that would better restrict the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing. **Perhaps, if there were meaningful judicial review and accountability, the FBI would take the statutory direction more seriously and actually implement it.**

147 Cong. Rec. at S10999 (emphasis added). Thus, as Senator Leahy explained, the additional privacy safeguards built into § 3121(c) were inserted because in practice the definitional sections were proving ineffective to stop law enforcement from over collecting and he wanted more "judicial review" and "accountability," and did not intend to loosen the restrictions on collecting PCTDD.

The goal of each amendment was to protect against the collection of contents of communications. There is no indication in the legislative history that any incidental collection of content was authorized.

SUMMARY OF ARGUMENT

FISA's plain language prohibits collecting PCTDD. FISA, by incorporating the definitions of "pen register" and "trap and trace" from 18 U.S.C. § 3127(3) & (4), defines PR/TTs as devices that do not collect content. 50 U.S.C. § 1841(2). The Government admits that PCTDD contains contents, and thus FISA does not allow its collection.

The Government's effort to use language limiting collection pursuant to PR/TTs authorized under Title 18 or State law is unavailing because that section, 18 U.S.C. § 3121(c), does not apply to PR/TTs authorized under FISA. Section 3121(c) applies only to government agencies authorized to install and use a PR/TT "under this chapter or under State law." FISA authorizations are not under chapter 206 of Title 18, but Chapter 36 of Title 50, and FISA does not incorporate § 3121(c) limitation into its own PR/TT provisions.

Even if § 3121 were applicable, it limits, not expands, the Government's ability to collect content under a PR/TT. The section is entitled "Limitation," and it places additional duties on law enforcement to use privacy-enhancing technologies to prevent overcollection. Reading § 3121 to limit, not expand, the government's ability to collect content is the simplest reading that gives effect to the plain text. It was enacted as a specific mandate to deploy technology to prevent the collection of contents under the broader scope of the new pen register statute, not to allow the government to incidentally collect contents of communications if technology to limit such collection is not reasonably available.

Moreover, Congress did not adopt the minimization and suppression scheme the Government imagines in FISA's PR/TT provisions (or in the criminal PR/TT statute). Unlike every other surveillance statute where Congress intended for such a scheme to apply, the PR/TT statutes contain no mention of minimization or

suppression. Compare 18 U.S.C. § 1842 with 18 U.S.C. § 2518(5) & 50 U.S.C. § 1805(c)(2).

Reading § 3121 as an additional privacy safeguard also harmonizes the statute. It effectuates the definitional limitations on the collection of content in § 3127(3) & (4) by imposing an additional duty on the government to use technology to ensure it does not collect content incidentally. The government's reading results in the reverse, creating a conflict with the statutory definitions and permitting it to do exactly what Congress sought to disallow.

Congress has consistently acted to prevent the government from doing what it seeks to do here, by repeatedly amending the PR/TT statutes to reinforce the requirement that PR/TTs cannot, by law, collect content. In 1986 it defined PR/TTs so they would be self-enforcing, believing (incorrectly) that the operation of such devices prevented the collection of content. In 1994, as technology changed, Congress enacted § 3121(c) specifically to eliminate the collection of content using PR/TTs. And again in 2001, when it discovered law enforcement had not complied with its intent, it enacted three separate provisions, each of which expressly commanded law enforcement not to use PR/TTs to collect content like PCTDDs.

The Government also ignores the elephant in the room. The ability to filter out all PCTDD, or limit its collection to certain digits, is a technological measure

reasonably available to it that prevents the collection of content. Under § 3121's plain command, it must use that technology or develop a better one.

Applying the Government's logic to other types of PR/TTs only highlights the flaws in its reasoning. In the Internet context, traffic sent through an ISP frequently contains a mix of content and non-content information—email addresses for routing and email contents are transmitted the same way. If the Government's logic were applied here, it could collect all Internet content and sort it out later, if it never developed technology to sort it prior to collection.

Finally, collecting PCTDD raises constitutional concerns under the Fourth Amendment. Individuals have an unmistakable privacy interest in PCTDD that includes financial or health information. The intrusion into these communications is not incidental, because the Government is intentionally collecting and targeting all PCTDD. And the minimization procedures the Government employs contain significant deficiencies. For example, they allow investigators to unmask PCTDD provided to any business entity. These provisions do not strike the right balance under the Fourth Amendment, because they allow the purposeful search and seizure of communications content without sufficient prior judicial review. This Court should, at a minimum, impose stricter minimization controls on collection, not just use, if it allows this practice to continue.

ARGUMENT

The FISC's custom of authorizing the recording and decoding of post-cut-through digits ("PCTDD") based primarily on the subsequent use prohibitions should be stopped. That practice goes against the weight of authority and reflects an incorrect interpretation of the statutes authorizing the use of PR/TTs in both the FISA and criminal context. Every other court to consider the issue in the form of a published decision has concluded that the government may not obtain PCTDD under PR/TT authority in Title III and the authority to do so under FISA pen register orders is no greater.[4]

A. The Plain Language of the Statute Prohibits the Collection of PCTDD that Contains Content.

This case should start and stop with the definitions of pen registers and trap trace devices, because each unambiguously prohibits collecting contents of communications, even temporarily. Robinson v. Shell Oil Co., 519 U.S. 337, 341 (1997) ("Our inquiry must cease if the statutory language is unambiguous and the statutory scheme is coherent and consistent."). Clear statutory text is the beginning and the end of the analysis. Barnhart v. Sigmon Coal Co., 534 U.S. 438, 450 (2002).

[4] The lone exception involved a case where the government obtained PCTDD from a provider, but immediately deleted all of the PCTDD upon receipt and did not seek to decode or retain it, even if it was purported to be non-content PCTDD. Garaufis, 632 F. Supp. 2d at 204.

The language is clear: pen registers are "a device or process which decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility…provided, however, **that such information shall not include the contents of communications**. . ." 18 U.S.C. § 3127(3) (emphasis added); 50 U.S.C. § 1841(2) (adopting § 3127(3)); Similarly, a "trap and trace device" is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, or 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 communications.**" (emphasis added). 18 U.S.C. § 3127(4); 50 U.S.C. § 1841(2).[5] FISA incorporates these definitions into its PR/TT provisions.[6]

These definitions are unambiguous: a device that records contents, even if only sometimes, is not a pen register or trap and trace device. See Orenstein, No. 08-mc-0595(JO), 2008 WL 5255815 at *3 (E.D.N.Y. Dec. 16, 2008). The definitions of pen register and trap and trace devices are foundational, and inform every subsequent use of those terms—including the lawful scope of a PR/TT order under

[5] These definitions find their roots in Smith, 442 U.S.at 745, which held that a pen register was not a search because pen registers "do not hear sound. They disclose only the telephone numbers that have been dialed – a means of establishing communication."

[6] The definition of trap and trace device includes the same prohibition against collecting the contents of communications. 18 U.S.C. § 3127(4).

50 U.S.C. § 1842. They ban "capturing" or "recording" content using pen register or trap and trace devices, and do not simply regulate the later use of information against a target. See United States v. New York Tel., 434 U.S. 159, 167 (1977); accord Smith, 442 U.S. at 741 ("[P]en registers do not acquire the **contents** of communication.") (emphasis in original); United States v. Rodriguez, 968 F. 2d 130, 135 (2d Cir. 1992) (same). The result is simple and clear. If a device captures content, it is by definition not a pen register or a trap and trace device.

The Government does not dispute that PCTDD, in many instances, can be content. (Gov. Br. at 13) ("Other post-cut through digits may constitute content, such as when a caller phones and is connected to an automated system, such as a financial institution or pharmacy, and, in response to prompts, enters digits that signify transferring funds from one account to another or a prescription number.") Because the devices here record PCTDD, which can include content, they are not pen registers and thus cannot be authorized under FISA.[7]

[7] The Government concedes that some PCTDD is content (i.e. financial account information) but argues that some PCTDD is not content. The majority of this brief addresses the legal analysis on the assumption that PCTDD can consist of both content and non-content. However, Section D of this brief offers an alternative reading of the statute that suggests *all* PCTDD is content, because once the call is cut through, the provider who is executing the pen register or trap and trace order is not using the additional information as dialing, routing or signaling information. Instead, as to that provider, all information post cut-through is considered content and is not intentionally disclosed to or used by the provider.

B. Section 3121(c) Does Not Apply to Pen Registers under FISA

The government seeks to justify capturing PCTDD based on a limitation on the use of pen registers authorized under Title 18 or State law, which FISA does not cross-reference or incorporate. Accordingly, based on first principles, it should not be part of this Court's analysis. FISA authorizes the government to apply to the FISC to obtain a pen register or trap and trace device for use in obtaining foreign intelligence information. 50 U.S.C. § 1842. FISA defines a "pen register" and "trap and trace device" to have the meanings given in 18 U.S.C. § 3127 (3) & (4), but does not incorporate all of the criminal code provisions related to PR/TTs. Nowhere does FISA refer to 18 U.S.C. § 3121(c) or any other sections of the pen register and trap and trace statute. Congress adopted only these definitions, leaving the rest to the scheme set forth in FISA's own pen register provisions.

Not surprisingly, the text of § 3121(c) limits its application to orders under that chapter, which does not include FISA. Section 3121(c) is not a part of the definitions under Title 18, but a limitation on a specific exception to the general criminal prohibition on the unauthorized use of PR/TTs for PR/TTs authorized under that statute or State law. *See* 18 U.S.C. § 3121 (Title) ("General prohibition on pen registers and trap and trace device use; exceptions") It provides that "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..." (emphasis added). FISA authorizes pen registers, but it is not located in Chapter 206 of Title 18. It is codified in Chapter 36 of Title 50. Rather than being part of the definition of a pen register, § 3121(c) is a specific limitation on pen registers authorized under Title 18 or State law, and no others.[8]

The Government and the FISC speed by this preliminary roadblock, stating that "[b]y giving a PR/TT obtained under FISA the 'meaning' of a PR/TT obtained under Title 18, section 1842(2) also incorporates the gloss on the meaning of a PR/TT supplied by section 3121(c)." (App. Br. at 8). But adopting the Government's argument would essentially re-write FISA to incorporate § 3121(c) explicitly into its definition of pen registers and ignore the language in § 3121(c) itself limiting the provision to pen registers issued "under this chapter or State law." If Congress intended to incorporate § 3121(c) into FISA, it could have done so initially, or in 2006 when it amended FISA. See USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006). Congress did not, and this Court should not expand its application by implication.

[8] There are other limitations placed in the statute authorizing criminal pen registers, which it appears that neither the government nor the FISC have applied in the FISA context, further underscoring that only the definitions sections have been imported into FISA. *See* 18 U.S.C. § 3123(a)(3) containing specific provisions that the government must follow when installing its own pen registers.

C. The Limitation in § 3121 Restricts the Government's Authority Rather than Expands It.

The "Limitations" provision of § 3121(c) does not authorize any governmental conduct – it restricts conduct. The Government's argument hinges on transforming the limitation in § 3121(c) into an expansion of the ability to collect content under PR/TT authority. But § 3121 specifically places additional duties on law enforcement to protect the privacy of communications by requiring the Government specifically to use technologies reasonably available (and not mere promises) to avoid collecting "the contents of any wire or electronic communications" when using a pen register. 18 U.S.C. § 3121(c); Azarack, 515 F. Supp. 2d at 330.[9] Rather than take it at face value, the Government loads § 3121(c) up like a Trojan horse—packing into it a free pass to collect all information it can and then sorting it out later. This reading has no basis in § 3121's text and is directly in conflict with the reasons why these provisions were added—to prevent the collection of communication contents.

The simple answer is that if the government cannot exclude contents, it cannot capture any PCTDD at all. See Smith, 441 F. Supp. 2d 816, 823 (S.D. Tex. 2006); Rosenthal, 622 F. Supp. 2d 411, 422 (S.D. Tex. 2007).[10] This uncomplicated

[9] Contents are defined as "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

[10] The Government appears to contend that the statute places an obligation on it to collect the maximum data allowed under the law. (See Gov. Br. at 29) ("the

reading is the correct one because: (1) Congress did not incorporate a minimization scheme into the PR/TT statute as it did in the Wiretap statute; (2) it harmonizes the provisions in section 3121(c) with the definitional sections rather than creating a conflict; (3) technology is and has always been available that serves to limit the collection of contents and the Government must use it; (4) it is more consistent with Congressional intent; and (5) it would cause substantial harm if applied in the context of an Internet pen register.

1. Congress Did Not Adopt a Minimization or Suppression Scheme

Unlike other surveillance statutes, Congress did not build a minimization or a suppression scheme into the pen register statutes, suggesting it did not authorize overcollection. Compare 18 U.S.C. § 3123 with 18 U.S.C. § 2518(5) (minimization) and 18 U.S.C. § 2515 (exclusionary rule). The Government repeatedly attempts to analogize pen registers to other surveillance laws that allow the Government to over-collect information if it later deletes or places use restrictions on the improperly acquired information. But no amount of bootstrapping can rewrite FISA's pen register statute to contain a minimization scheme that Congress left out of the criminal pen register statutes and FISA, but expressly included in other surveillance statutes. The word "minimization"

---

government must collect all post cut through digits to obtain the DRAS authorized by statue.") This mandatory collection is nowhere in the statute.

appears only once in FISA's pen register provision—in a rule of construction that allows the Attorney General to impose *additional* privacy or minimization procedures for the use of pen register or trap and trace devices. 50 U.S.C. § 1842(h)(2). But this provision, which allows the Attorney General to minimize the use of *non-content* data collected using a PR/TT and provide *additional* privacy protections, should not be read to *expand* the Government's ability to collect information using a FISA PR/TT.

Instead, FISA's PR/TT authority repeatedly specifies that pen registers and trap and trace devices cannot collect content in the first place. It adopts the definitions of pen register and trap and trace from the criminal pen register statute, which each specifically state that those devices shall not collect content. 50 U.S.C. § 1841(2).[11] And no provision in § 1842 contemplates the collection of content and subsequent minimization or suppression of it.

---

[11] The 2006 amendment to FISA lists data that a provider may be compelled to provide on request—but the amendment related to *stored* customer information like a subscriber name, network address, telephone records, and mechanisms and sources of payment, not the real time DRAS that a pen register collects. 50 U.S.C. § 1842(d)(2)(C). The government's brief implies that this new section expanded the scope of authority for pen register collection (Gov. Br. at 8), but the legislative history makes clear that this section was intended to allow FISA pen registers to let the government simultaneously demand historical information about the subscribers whose numbers appeared in the pen register results. This, it was designed to mirror the types of stored records available under 18 U.S.C. § 2703(d), which addresses stored data, not real-time collection. USA PATRIOT Reauthorization Act, S. Rep. 109-85 at 25 ("This provision is modeled on 18 U.S.C. § 2703(c)(2) and (d).")

When Congress has intended to adopt a minimization or suppression scheme, it has done so expressly. FISA and the criminal PR/TT statutory text stand in stark contrast to the Wiretap Act, which specifically permits the government to "over collect" and then apply minimization procedures to eliminate the collection of unauthorized content. 18 U.S.C. § 2518(5). "The [Wiretap] statute does not forbid the interception of all nonrelevant conversations, but rather instructs the agents 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); see also 50 U.S.C. § 1805(c)(2) (directing that minimization procedures be followed); 50 U.S.C. § 1801(h)(1) (same).

FISA's PR/TT authority, on the other hand, contains no such provision. And "minimization" is conspicuously absent from § 3121. As Courts have found "unlike the Wiretap act, the Pen Register Statute does not contain an obligation to minimize the collection of the content of communications; it contains an affirmative obligation *not* to collect in the first place." Rosenthal 622 F. Supp. 2d at 422 (emphasis in original). The Government should not be able to read such a scheme into FISA's PR/TT statute by mere association with other surveillance statutes that have distinct statutory language.

2. Reading § 3121 as a Limitation Harmonizes the Statutes.

Reading § 3121(c) as an additional privacy safeguard designed to further restrict the collection of contents best harmonizes § 3121(c) with § 3127(3) & (4). See Food & Drug Admin. v. Brown & Williamson Tobacco Corp., 329 U.S. 120 (2000) (holding that a court should interpret a statute as "a symmetrical and coherent regulatory scheme and fit, if possible, all parts into a harmonious whole.") The government's reading, by contrast, creates conflict. If the government can collect all PCTDD, including some content, simply because "no reasonably available technical procedures" are available to it, it clashes with the prohibitions on collecting content using a PR/TT and the commandment to use reasonably available technology from the statute. If the government cannot separate PCTDD contents from non-content, then it must apply the reasonably available means of *not collecting PCTDD* to avoid the collection of content in the first place.[12] As Judge Smith rightfully declared, "[i]f the government believes that pen register technology is too restrictive, then the correct response under the statute is to develop better technology, not ignore the statutory command." Smith, 441 F. Supp. 2d at 825; see also Rosenthal, 622 F. Supp. 2d at 422 (finding that the government is precluding from collecting content at all, even if some non-content goes uncollected).

[12] Again, limiting collection to a specific number of digits is a reasonably available technology, and always has been.

Section 3121(c) does not, as the Government suggests, direct it to merely minimize the collection of content, but allow the collection of non-content. Instead, § 3121(c) allows the Government to use technology to maximize the collection of all forms of non-content, so long as it preserves the prohibition on collecting content. Smith, 441 F. Supp. 2d at 824-25. It is consistent with the definitions in § 3127(3) & (4) because the Government may use technological means to maximize the non-content it can collect when using a pen register or a trap and trace device, but it cannot do so at the price of collecting content.

Interpreting § 3121(c) as maximizing collection of non-content, rather than allowing collection of content and minimization is consistent with interpreting § 3121(c) as what it says it is: a "Limitation." Section 3121 is not designed to authorize additional surveillance powers. It is entitled "Limitation." It was expressly intended to restrict collection, not enable it. It imposes an affirmative obligation for the government to do *more* not to collect content, *not* to do less.

The Government's reading is the reverse, and creates a significant tension between express language *prohibiting* the collection of content in the definitions of pen registers, trap and trace devices, and the final sentence of § 3121(c). Each provision specifically emphasizes that a PR/TT shall not "include the contents of any wire or electronic communication." To avoid creating tension, the Government would have to rewrite § 3121(c) to allow for collection and

minimization of content, which would be a fundamental change to the intended statutory regime. But Congress does not hide elephants in mouse holes. Whitman v. Am. Trucking Ass'ns, 531 U.S. 457 (2001) ("Congress, we have held, does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions –it does not, one might say, hide elephants in mouseholes.")

3. Congress Intended to Prevent the Collection of Content

Congress has had numerous opportunities to amend the PR/TT statutes to allow for the collection of PCTDD, but it has done the opposite, repeatedly amending the statute to make clear that the government *cannot* collect any content using PR/TT authority. In 1986, Congress defined pen registers in ECPA narrowly, believing that they would not be able to record anything more than information used to route calls. In 1994, Congress became aware this was not the case, and added 18 U.S.C. § 3121(c) to address Senator Leahy's specific concerns that law enforcement was now able to impermissibly collect content using a pen register. 103d Cong., 2d Sess. 50 (March 18, 1994).

Again in 2001, when Congress passed the USA PATRIOT Act, it learned that law enforcement was still collecting contents using pen registers. It modified the definition of pen register to specify that PR/TT devices could not include "the contents of any communication." As Sen. Leahy stated, he was "concerned about the FBI and Justice Department's insistence over the past few years that the

pen/trap devices statutes be updated with broad, undefined terms that continue to flame concerns that these laws will be used to intercept private communications content." 147 Cong. Rec. at S11000. He also wanted to subject the government's actions to greater judicial review and oversight, not less, because he believed that the FBI was acting unconstitutionally in collecting content with a Pen Register:

> When I added the direction to use reasonably available technology (codified as 18 U.S.C. § 3121(c)) to the pen register statute as part of the Communications Assistance for Law Enforcement (CALEA) in 1994, I recognized that these devices collected content and that such collection was unconstitutional on the mere relevance standard. Nevertheless, the FBI advised me in June 2000 that the pen register devices for telephone services 'continue to operate as they have for decades' and that 'there has been no change that would better restrict the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing. **Perhaps, if there were meaningful judicial review and accountability, the FBI would take the statutory direction more seriously and actually implement it.** Id. (emphasis added)

As Judge Azrack recognized, "Senator Leahy's recognition that collection of content is unconstitutional is important. We must assume Congress would not want to enact unconstitutional provisions ... and there is no indication of Congressional intent to the contrary." Azarack, 515 F. Supp. 2d 325, 333 (E.D.N.Y. 2007). The government's reading thus flies in the face of this clearly expressed statutory intent. Having amended the statute in multiple different ways to put an end to the collection of any PCTDD that qualifies as content, Congress could hardly have done more to avoid precisely the result the government seeks.

4. Technology is Available to Limit the Collection of Content

The government ignores the elephant in the room: its ability to use existing technology to not collect PCTDD. In doing so, the Government fails to address why excluding PCTDD from collection based on the number of digits is not a reasonably available technology. As the Government points out, the statute does not specifically mention PCTDD (Gov. Br. at 28), so it certainly cannot command the Government to collect it. But it does command the government to use technological measures—not to use them only if they are reasonably available. See 18 U.S.C. § 3121(c) ("shall use technology reasonably available"). There is no "if" in the law. Configuring a pen register to avoid collecting PCTDD entirely is a reasonably available technical measure. And the Government admits that it has that technology. As a Department of Justice Manual states:

> **Caveat. Technology is available** to limit the pen register device so that it only records a specified number of dialed digits, for example, the first 10 digits ... [Doing so would] eliminate the inadvertent collection of 'content' of a communication....

R. Stabe, Electronic Surveillance – Non-Wiretap, at § 3.4, in Federal Narcotics Prosecutions, quoted in Smith, 414 F. Supp. 2d at 825 (emphasis added). The government *can* use technology to limit collection currently, even though some non-content is left uncollected.

The Government's argument is that a technology is reasonably available only if it allows the Government to collect *all* non-content PCTDD. And absent such

technology, the law requires it to do nothing. But reasonably available does not mean perfectly suited for the government's objectives. Instead, if the Government thinks that the technological ability to collect non-content PCTDD is insufficient to meet investigative needs, then it must use what technology it has available while it takes on the task of improving it.[13]

The Government's reading also incentivizes the Government never to build technology to sort PCTDD during collection because in the absence of technology, the Government can collect all data and sort it out later. It is not reasonable to assume that Congress passed a limitation on the Government's ability to collect information under a PR/TT that would be "a mere contingency, lying dormant until some future day when a foolproof filter is found." Smith, 441 F. Supp. 2d at 825. If the technology reasonably available—even if it is simple and crude, like limiting collection to the first 10 digits dialed or not collecting PCTDD—is not good enough, the Government should not reap the benefits of its own inability to do better. As Judge Smith recognized, "The Government's position ... gives no

[13] Indeed, there are likely other reasonable measures that can be used. For example, the government can develop and maintain a list of known calling service numbers and the PCTDD can be compared to the list of known calling service numbers. If the pre-cut through dialed digits match a number on the list, the post cut through numbers are collected or provided. In the Internet context, similar technology allows websites to check IP addresses against a list of known proxy servers on the fly, and block requests from those proxies. See, e.g., Maxmind, Proxy Detection Web Service, available at http://dev.maxmind.com/proxy-detection. (last visited Mar. 25, 2016)

incentive to anyone in government or industry to alter the technological status quo, which perhaps explains why there is no effective filtering technology 12 years after CALEA decreed its use." Id. at 825-26. It is now 22 years since CALEA, and according to the Government, that technology, predictably, still does not exist. Had the government been required to develop the technology sooner, it is unlikely there would be so many fallow years of development.

5. The Government's Logic, if Applied to an Internet Pen Register, Would Cause Substantial Harm

The flaw in the government's approach can be readily seen if the same logic were to be applied to Internet pen registers.[14] [redacted] b3 Per FBI b7E

[redacted]

[redacted] b3 Tammie b7E

[redacted] This cannot be the correct interpretation of the statute.

Such collection on the Internet would be directly contrary to Congressional intent in expanding the pen register statute to the Internet. See H.R. Rep. No. 107-36 at 33 (stating that a pen register order could not be used to collect "the portion of a URL specifying web search terms or the name of a requested file or article."); See In re Zynga Privacy Litig., 750 F.3d 1098, 1108-09 (9th Cir. 2015) (some if not most queried URLs are content). It would also clearly implicate serious Fourth Amendment concerns. Riley v. California, 134 S.Ct. 2473, 2490 (2014) (stating that Internet search and browsing histories could reveal an individual's private interests or concerns). Thus, the government's statutory interpretation presents a problem of a significantly greater magnitude if applied to the Internet as it would allow the capture of vast quantities of private communications under the authority

of a pen register. See In re Application of the United States, 396 F. Supp. 2d 45, 47-49 (D. Mass. 2005) (pointing out the greater problem with overcollection in the Internet context). As examined in the Internet context, the fallacy of the government's statutory interpretation becomes readily apparent.

D. Alternatively, PCTDD Should be Considered Content to the Provider

Alternatively, the court should deeply consider the question raised by the D.C. Circuit in U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 462 (D.C. Cir. 2000) as to whether all PCTDD should be considered content for purposes of the PR/TT statutes and therefore should be obtained only through an electronic surveillance order.[16] For purposes of the PR/TT statutes, content is defined as set forth in 18 U.S.C. §2510 as ("any information concerning the substance, purport, or meaning of that communication.") The government and the court below have assumed that there are specific types of PCTDD that fall into the category of dialing, routing and signaling information ("DRAS") even though the provider who has received the PR/TT order does not itself use the information for dialing, routing or signaling purposes. *See* Certification Order at 3 ("in the calling-card example, the post cut-through digits are non-content DRAS information") But it is not clear that this is

[16] See U.S. Telecom Ass'n, 227 F.3d at 462 ("It may be that a Title III warrant is required to receive all post cut-through digits.") The Court need not reach this issue if it finds that the collection of PCTDD that undisputedly contains content is unauthorized.

the case. Once a call has been "cut-through," any additional digits that are pressed by the user are communications that neither intended for nor used by the provider who has received the PR/TT Order.[17]

The pen register statutes were initially passed as result of Smith v. Maryland, in which the Supreme Court held that users did not have a reasonable expectation of privacy in dialed digits knowingly conveyed to the phone company to route calls. Specifically, the court stated that:

> All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. In fact, pen registers and similar devices are routinely used by telephone companies [for their own purposes]

Id. at 742.

None of this is true with regard to PCTDD in the hands of the initial phone company. Here, AT&T does not use the PCTDD to connect or route calls, does not maintain it on its bills, does not use it for its own purposes, and would not capture it at all but for the law enforcement command. Nor does the user believe

[17] Although the record is unclear, this view may have been shared at one time by the Justice Department in 1998 when it advised then-House Judiciary Committee Chairman Henry Hyde that "all of the information transmitted after a phone call is connected to the called party . . . is substantive in nature. These 'electronic impulses are 'contents' of the call. They are not used to direct or process the call, but instead convey certain messages to the recipient." 147 Cong. Rec. at S11000.

the PCTDD are being disclosed to AT&T, regardless of whether they relate to financial accounting transactions, airline reservations or subsequent calls. The user expects that the communications are only being disclosed to the ultimate recipient, in the same way that the user was not knowingly broadcasting his phone call in Katz, notwithstanding the fact that telephone company had the ability to monitor the calls. See Katz v. United States, 389 U.S. 347, 352 (1967). And for the same reason that the government cannot distinguish between PCTDD that relates to a financial transaction as opposed to that which relates to a subsequent call, AT&T cannot do so either.[18] Thus, to the provider who is being asked to provide the PCTDD to the government, it is an interception of call content, not dialing, routing or signaling information,[19] because the call has already been routed. Surely this would be the case where the subsequent commands were verbalized to an IVR (Integrated Voice Response) system. Such spoken word commands, whether to "change reservations" or "initiate conference call," could not be captured merely by a PR/TT served on AT&T. Yet, the government is asserting that because

[18] Indeed, without an order or another statutory exception AT&T could risk potential criminal sanction and civil liability for intercepting PCTDD under the Wiretap Act. See 18 U.S.C. § 2511.

b3 Per FBI
b7E

certain commands sent over AT&T's lines cause a subsequent third-party to initiate a non-call transaction, the government should still be able to collect all such commands to decode them.[20]

[redacted] b3 b7E

[redacted] The same should be considered true for PCTDD that are not normally captured by and used by AT&T for dialing, routing, or signaling.

[20] The government does not yet seek the right to intercept any subsequent voice commands to decode only the ones that are being used to command a third-party system to initiate a third party call, but it would seem that its logic would allow it to do so. If it does not, then bad actors can simply use third-party calling systems that accept voice in addition to, or in lieu of digit commands.

E. Collection of PCTDD Raises Constitutional Concerns That Have Not Been Adequately Addressed[21]

In all circumstances, collection of PCTDD raises constitutional concerns that are not adequately addressed by the government's current minimization practices. This is true whether all or just a subset of PCTDD is considered to be content. The government does not dispute that users have a reasonable expectation of privacy in certain types of PCTDD that are not phone numbers or DRAS, but argue that its current "extraordinary" minimization efforts meet the Fourth Amendment standard of reasonableness. (Gov. Br. at 15, 50) *Amicus* disagrees.

1. Individuals have a Privacy Interest in Certain Types of PCTDD

The government concedes that some PCTDD entered into touch tone response systems are contents of communications. As automated response systems now collect information that used to be spoken over the telephone, it cannot seriously be disputed that the transmission of social security numbers, financial account numbers, prescription information and birthdates by PCTDD rather than by voice is entitled to Fourth Amendment protection. And tracking this information over time, as a pen register does, is more intrusive than an isolated capture. See Riley, 134 S.Ct. at 2489. Use of telephones to transmit this information is part of an individual's "subjective expectation of privacy that

[21] The Court does not need to reach this issue if it determines that the collection of content PCTDD is beyond the statutory authority of 50 U.S.C. § 1842.

society recognizes as reasonable." Kyllo v. United States, 533 U.S. 27, 33 (2001); Katz, 389 U.S. at 361.

2. FISA's Pen Register Provisions Provide Too Little Protection of Privacy Interests.

Amicus does not dispute the weight of the governmental interest in national security, nor can it quarrel with the applicability of the special needs analysis as a basis to allow the government to collect certain foreign intelligence information without first obtaining a warrant based on probable cause. See In re Directives Pursuant to Section 105B of the For. Intel. Surv. Act, 551 F.3d 1004 (FISA Ct. Rev. 2008) (finding that foreign intelligence surveillance qualifies under the special needs analysis). But, the question remains as to whether the collection of PCTDD pursuant to the government's internal minimization procedures is reasonable under the Fourth Amendment. That analysis requires the Court to assess "the degree to which [a search] intrudes upon an individual's privacy and ... the degree to which it is needed for the promotion of legitimate government interest." United States v. Knights, 534 U.S. 112, 118-19 (2001).

The government's collection of content-based PCTDD is a search within the meaning of the Fourth Amendment. United States v. Jacobsen, 466 U.S. 109, 113 (1984) (holding that a search occurs when the government infringes upon 'an expectation of privacy that society is prepared to consider reasonable.'). The

intrusion into privacy here is more than minimal.[22] The information that the government will be obtaining—despite being "a string of digits"—is a meaningful string of digits that in some cases will be a password, social security number, travel reservation, financial account number, or pharmaceutical prescription. Typically, financial and health information are treated as the most sensitive types of information under U.S. law and entities who process and store it are subjected to a salmagundi of privacy and security obligations. See Health Portability and Accountability Act of 1996, P.L. 104-171, 110 Stat. 1938 (1996); Gramm-Leach-Bliley Act of 1999, P.L. 106-102, 163 Stat 1338 (1999).

Yet, to obtain such confidential and private information, the threshold showing needed under FISA's pen register statute is minimal, and leaves the judge with little power to review or deny an application. An application for a PR/TT under FISA must contain only three elements, one of which is the name of the officer seeking to use the PR/TT and the selection term to be targeted (such as a phone number). 50 U.S.C. § 1842(c)(1) In addition to a name and a target, FISA requires that the applicant certify that "the information likely to be obtained is foreign intelligence information not concerning a United States person or is

[22] The government's contrary contention – that the digits obtained from the pen register are unlikely to reveal any personal information about the individual is surprising and seems premised on the government not taking the minimal steps required to decode it. *See* Gov. Br. at 53-54.

relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities." *Id.* § 1842(c)(2). Once the FISC receives the application, its review is limited. FISA states that the judge "shall enter" an order approving the use of the PR/TT and it provides no standard for reviewing the government's certification of relevance. *Id.*§ 1842(d). This is not the type of rigorous scrutiny that is a reasonable substitute for a warrant. In Directives, 551 F.3d at 1013 ("the more a set of procedures resembles those associated with the traditional warrant requirements, the more easily it can be determined that those procedures are within constitutional bounds") citing, In re Sealed Case, 310 F.3d 717, 742 (FISA Ct. Rev. 2002).

3. The Government's Collection of PCTDD Content is Intentional, Not Incidental.

The Government characterizes the collection of content using a pen register that collected content-based PCTDD as "incidental to its collection of non-content post-cut through digits." (Gov. Br. at 50), but there is nothing incidental about the collection here. In In re Directives for instance, the incidental collection was the collection of U.S. person's communications while conducting authorized surveillance on non-U.S. persons located abroad. In that case, the targets were exclusively foreign persons, and any collection of U.S. persons' communications would be happenstance. Here, the Government is intentionally targeting and collecting content-based PCTDD because it *might* contain non-content

information. While amicus does not have access to evidentiary information, it is possible that content PCTDD constitutes the bulk (or a significant portion) of all PCTDD.[23] In the context of the In re Directives case, it would be as if the Government is collecting U.S. person's communications because it knew that those communications sometimes contained non-U.S. person's communications, and "minimizing" the use of U.S. person's communications.[24]

4. The Government's Collection of PCTDD is Not Necessary.

The second part of the balancing test is determining "the degree to which it is necessary for the promotion of legitimate government interests." Knights, 534 U.S. at 118-119. Here, the Government has other means by which it can obtain the information it seeks. Declining to authorize a collection and minimization scheme that was not intended by Congress does not deprive the government of the ability to collect valuable data that is important to national security investigations. First, the government can use the same PR/TT authority on the subsequent provider of

---

[23] The court should consider inquiring as to whether the majority of PCTDD entered by U.S. phone users is of the content, or non-content variety. Given the prevalence of automated phone response systems for all aspects of U.S. citizens daily life, it would be surprising if calling card services were called more than airlines, banks, and customer service numbers.

[24] Moreover, in In re Directives, the court noted that the government assured the court that it did not create and maintain a database of the incidentally collected communications received from non-targets. In re Directives, 551 F.3d at 1014-15. But here, all PCTDD is specifically maintained in one or more databases, even if not used without subsequent permission.

calling services. That is, when a target dials a number that is identified to be a calling service within the jurisdiction of the U.S. or its allies, the government can seek to obtain a second round of process to obtain the dialing, routing and signaling information from the subsequent communications provider. Second, the government can use surveillance authority under Title I of FISA (50 U.S.C. § 1801, et seq.) to obtain authority to intercept the full content of communications, including the PCTDD. Third, the government can pursue the course that Congress intended in 2001 to develop technological solutions that would allow for a greater collection of non-content PCTDD without capturing the types of PCTDD that is beyond the reach of the PR/TT statute.[25]

5. The Minimization Requirements Do Not Suffice

The minimization procedures employed by the government are insufficiently protective given the ubiquity of automated response systems. The government's key argument here is that the minimization procedures it employs should tilt the scales in favor of upholding its actions. See In re Directives, 551 F.3d at 1012.

[redacted]

b3 Per FBI
b7E

[25] The fact that there have been no developments in this area over the past decade is surprising given the pace of technological solutions in other aspects of the industry and is certainly suggestive of the fact that there may be no incentive to develop such solutions so long as post-collection decoding and minimization are considered to be adequate in the types of cases for which there is high demand and available funding.

[redacted] b3 Per FBI b7E

Furthermore, although *Amicus* does not have access to consult third-parties for technology solutions, there may be other reasonable steps that are within the power of the FISC to order to reduce the privacy intrusion after collection. For instance, in this case, the government is interested in how target uses domestic and foreign calling services to place subsequent calls. It is unclear why the government could not use a post-processing script to delete all PCTDD for all calls that are not made to known calling services, or to create scripts that can identify phone number formats in strings of dialed digits using known country codes—particularly for the specific countries the target dials, and delete all other PCTDD.

[26] It is of not much help that it must be reasonable to believe that the PCTDD related to a business entity must contain dialing or signaling information, because in the hotel example the government offers, a call to a business could involve a request to be transferred to a specific extension. See Gov. Br. at 56. It also might involve the content of private transactions.

Amicus suspects that there are a variety of technological means short of collecting no PCTDD that the government could develop—but that the government does not consider them reasonable simply because they would eliminate some PCTDD. But at bottom the statutory commandment is to "not collect contents," not to "collect all non-content PCTDD." Thus, while current technology may be not be perfect, whatever technology is available *must be used* to prevent the government from collecting the contents of communications, even if some non-content information cannot be collected.

The facts of this case demonstrate the need for greater safeguards with regard to PCTDD. [redacted] b3 Per FBI b7E

[redacted]

[redacted] A more relevant statistic is how many of the numbers dialed pertain to known calling card services. If the government cannot determine how many of the

[redacted] there is no basis to determine that they contain DRAS within scope of the pen register statute. b3 Per FBI b7E

To the extent that the Court allows the continued collection of PCTDD that may contain contents, despite the statutory mandate to do otherwise, the Court should remand this case to the FISC so it can use its supervisory authority, specifically reserved under 50 U.S.C. § 1842(h)(2), to impose additional privacy and minimization procedures on the collection and retention of PCTDD.

March 28, 2016

By: _____

Marc J. Zwillinger
Amicus Curiae
ZwillGen PLLC
1900 M St NW, Suite 250
Washington, D.C. 20036
marc@zwillgen.com
Tel: (202) 706-5202

Jacob A. Sommer
ZwillGen PLLC
1900 M St NW, Suite 250
Washington, D.C. 20036
jake@zwillgen.com
Tel: (202) 296-3585

CERTIFICATE OF COMPLIANCE

This brief complies with the relief requested in *Amicus*'s motion to file an oversized brief because it contains 10,897 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in 14-point font size and Times New Roman type style.

March 28, 2016

By: _____

Marc Zwillinger
ZwillGen PLLC
1900 M St NW, Suite 250
Washington, D.C. 20036
Telephone: (202) 296-3585
Facsimile: (202) 706-5298

~~SECRET//ORCON/NOFORN~~

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

IN RE CERTIFIED QUESTION OF LAW.	Docket No: FISCR 16-01

CERTIFICATE OF SERVICE

Pursuant to FISCR Rule of Procedure 16, on March 28, 2016, I provided five true and correct copies of Amicus's Brief to [redacted] Legal Advisor to the Foreign Intelligence Surveillance Court, who has informed me she will deliver an original and three copies to the Court for filing, and one copy to:

[redacted]
Chief, Counterintelligence Unit
Office of Intelligence
National Security Division
United States Department of Justice
950 Pennsylvania Ave. NW
Washington, D.C. 20530

March 28, 2016

By: _____

Marc Zwillinger
ZwillGen PLLC
1900 M St NW, Suite 250
Washington, D.C. 20036
Telephone: (202) 296-3585
Facsimile: (202) 706-5298