No. 16-

In the
Supreme Court of the United States

An Unknown United States Person

v.

The United States of America

On Petition of a Writ of Certiorari, or a Writ of Error, to the Foreign Intelligence Surveillance Court of Review

Petition for Review by Amicus

Steven Presser
Michael Walsh
John Walsh
Counsel of Record
Walsh & Walsh LLP
PO Box 9
Lynnfield, MA 01940
617-257-5496
Walsh.lynnfield@gmail.com

Questions Presented

In the Foreign Intelligence Surveillance Court of Review's third ever published case the Court of Review held that the government may record and store, post-cut through digits ("PCD") of a telephone call. PCD data are telephone digits dialed after a phone call is connected to a source, which may include bank information, credit card digits, or further routing information such as telephone extensions or calls put through by an operator. Some of this information the Government concedes is protected content information and other information is meta-data which the Government may access under this Court's decision in *Smith v. Maryland*, 442 U.S. 735 (1979). Applying a novel "foreign intelligence exception" to the Fourth Amendment, which this Court had previously declined to recognize, the Court of Review allowed the Government access to PCD, covering content information, upon the theory that the technology is not yet available to distinguish between content digits and additional routing information.

1. Whether the Court of Review erred balancing the Fourth Amendment reasonableness of government access to PCD without probable cause or warrant, by erroneously applying a "foreign intelligence exception" not recognized by this Court and contrary to the holding in *United States v. United States District Court*, 407 U.S. 297 (1972) (the "Keith case").
2. Whether the asserted technological incapability is a legally sufficient basis to

invade PCD content information protected under the Fourth Amendment

Table of Contents

Table of Authorities

Statutes

List of the Parties/Corporate Disclosure

The United States of America is a sole party participating. The litigation centers on a specific unnamed U.S. person, who has not participated in the litigation and may not been notified of ongoing surveillance. The Court of Review appointed an *amicus curie* who opposed the Government's position before it. The present would-be amicus seeks to press the argument before this Court.

None of the parties have a corporate existence or parent companies.

Opinions Below

On January 21, 2016, in *In Re: [Redacted], A United States Person*, Judge Hogan of the Foreign Intelligence Surveillance Court ("FISC") granted a Government application for a Pen Register and Trap and Trace device. After subsequent briefing, the FISC opted to certify questions of law regarding government access to PCD data, because FISC practice differed from most other federal courts. (*Infra,* App. 39-41) On consideration of the certified questions, the Foreign Intelligence Surveillance Court of Review ("FICOR") issued an opinion on April 14, 2016, Docket 16-01. (*Infra,* App. 33-34) The decision was not approved for declassification by the Director of National Intelligence until August 18, 2016. *Id.* The decision was not published until August 22, 2016. The decision of FISC and FICOR in this case are published on their website. FISC Decision (http://www.fisc.uscourts.gov/public-filings/certification-question-law-foreign-

intelligence-surveillance-court-review) and FICOR Decision (http://www.fisc.uscourts.gov/public-filings/opinion)

Statement of Jurisdiction

This Court has jurisdiction to review decisions of the Foreign Intelligence Surveillance Court of Review under 28 U.S.C. § 1254 and to issue an appropriate writ of error under 28 U.S.C. § 1651. The Foreign Intelligence Surveillance Act further provides a series of interlocking statutes authorizing this Court's jurisdiction. 50 U.S.C. § 1803(b)(jurisdiction upon certiorari appeal by United States); §1803(f) (power of Supreme Court to modify orders); §1803 (k) (authorizing this court to review certified questions); § 1861(f)(3) (jurisdiction over production and nondisclosure orders); §1881a(h)(6)(B) (jurisdiction over directives to service providers targeting persons not in United States); §1881a(i)(4)(D) (jurisdiction for judicial review of minimization and targeting procedures on application of United States). The Court also has jurisdiction under its general supervisory power over Federal Courts.

Statutory and Regulatory Provisions Involved

Relevant statutes and regulations involved in this proceeding are reproduced in the Appendix.

Statement

In 1978, following the Church Committee Report, the Rockefeller Commission Report, public

disclosure of the Central Intelligence Agency's "family jewels," and the widespread abuse of bugging by the Nixon Administration under the fraudulent guise of national security, Congress enacted the Foreign Intelligence Surveillance Act of 1978 ("FISA"). 50 U.S.C. § 1801, *et seq.* FISA was substantially amended by the USA PATRIOT ACT of 2001, following the terrorist attacks on September 11, 2001. The modern history of the FISA Act begins with the disclosure by the New York Times on December 12, 2005, that the President had unilaterally authorized extra-judicial wiretapping which circumvented the FISC. Following a negative decision by FISC that remains classified, Congress passed the Protect America Act of 2009 ("PAA") which, among other things provided new surveillance powers to the Government. Some of the provisions of the PAA were reversed the following year in the FISA Amendment Act of 2008, although the 2008 Act extended an immunity from suit to telephone carriers who cooperate with the Government.

In June 2013, fugitive Edward Snowden, formerly a contractor for the National Security Agency, revealed widespread mass surveillance by the Government to the Guardian Newspaper. Among the first items disclosed by Mr. Snowden was a routine re-authorization from the FISC for the large-scale collection of "telephony meta-data" under Section 702 of the FISA statute. After subsequent public outrage, Congress debated surveillance heavily. A filibuster of a reauthorization bill by Senator Rand Paul of Kentucky allowed the post-Patriot Act surveillance

authorization to expire for roughly 24 hours on June 1, 2015. Subsequently Congress enacted the USA FREEDOM ACT, a surveillance reform measure.

The individual in this case is unknown and the details remain classified. All that is publicly known is that he/she is a U.S. National. The Government applied for a pen register authorization to tap a cell phone. Pen Registers and Trap and Trace Devices do not generally collect information except for dialed digits or characters.

Reasons for Granting the Petition

1. The Decision Below is novel—First Major Application of Foreign Intelligence Exception to Fourth Amendment

So far as the public record discloses, this Court has never reviewed any decision of FICOR. In part this is due to the scarcity of such decisions, there only being two prior decisions of FICOR in its 38 year history. *In Re: Sealed Case*, 310 F. 3d 717 (FICOR 2002); *In Re: Directives*, 551 F.3d 1004 (FICOR 2008). The current decision is the first substantial exposition of, and concrete application of, a so-called foreign intelligence exception to the Fourth Amendment. FICOR recognized the exception, but did not explore its boundaries, in 2008. 551 F.3d at 1010-1012.

Several lower federal courts have adopted a foreign intelligence exception to the Fourth Amendment, but almost all that have done so did so before the

enactment of FISA in 1978. *United States v. Bin Laden*, 126 F.Supp.2d 264, 272 n.8 (SDNY 2000). *Cf In Re: Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157, 172 (2nd Cir. 2008) (declining to adopt foreign intelligence surveillance exception, but declining extraterritorial application of Fourth Amendment). "FISA, enacted in 1978, was Congress's response to judicial confusion over the existence, nature and scope of a foreign intelligence exception to the Fourth Amendment's warrant requirement in the wake of the Supreme Court's 1972 decision in *United States v. U.S. District Court*, 407 U.S. 297, 92 S.Ct. 2125, 32 L.Ed.2d 752 (1972)." *United States v. Sherifi*, 793 F.Supp.2d 751, 753 (E.D.N.C. 2011). The confusion about the scope of the exception, if it still exists after the enactment of FISA, is murky at best.

The modern Fourth Amendment stands on two pillars—the Warrant Requirement and Probable Cause. The Fourth Amendment generally requires both elements, but depending upon context may dispense or alter either. In the administrative search context, this Court has normally required search warrants even where no individualized showing of probable cause is required. *City of Los Angeles v. Patel*, 135 S.Ct. 2443 (2015); *Camara v. Municipal Court*, 387 U.S. 523 (1967) (municipal inspection regime subject to warrant requirement even if probable cause standard altered); *Marshall v. Barlows, Inc.*, 436 U.S. 307, 320 (1978) ("Probable cause in the criminal law sense is not required" but a warrant may still be required). The converse is also true, that probable cause (or its cousin reasonable suspicion) may meet the Fourth

Amendment's requirements without a warrant. This is prevalent in the exigent circumstances exception, the automobile exception, and the search incident to lawful arrest.

The Fourth Amendment embodies several different interests and protections. The requirement of a neutral and detached magistrate, reviewing each individual case, safeguards against excessive and unnecessary invasions of privacy. The probable cause requirement induces the Government to assemble a likely case of individualized misconduct. The Warrant itself confines the discretion of the searching officer and circumscribes the scope of the search or seizure. Even the requirement of an affidavit or oath by the applicant serves to put the government officials on their word and honor before they may invade and interfere with a citizen's private life. Many of the concerns, such as the particularity requirement, focus on separation of powers concerns about confining the discretion of the Executive.

Even when this Court has "carved out carefully delineated exceptions" to the textual dictates of the Fourth Amendment, there have always been careful limitations. "Our decisions [] cannot be taken as establishing a freewheeling authority to declare new categories of [searches] outside the scope of the F[ourth] Amendment." *United States v. Stevens* 130 S.Ct. 1577, 1586 (2010).

When the stakes are highest, that is the most important time for Government to be held to its burden. Generalized and vague claims of national

security do not dispense with the Constitution or its strictures. *Keith,* 407 U.S. at 314. The history of dictatorship shows that claims of national security all too often serve as cloaks for egregious human rights abuses, governmental overreach, mass surveillance, and other adornments of totalitarianism.

> The Fourth Amendment is a restraint on Executive power. The Amendment constitutes the Framers' direct constitutional response to the unreasonable law enforcement practices employed by agents of the British Crown… Over the years — particularly in the period immediately after World War II and particularly in opinions authored by Justice Jackson after his service as a special prosecutor at the Nuremburg trials — the Court has recognized the importance of this restraint as a bulwark against police practices that prevail in totalitarian regimes

California v. Acevedo, 500 U.S. 565, 586 (1991) (Stevens, J. dissenting). "But the forefathers, after consulting the lessons of history, designed our Constitution to place obstacles in the way of a too permeating police surveillance, which they seemed to think was a greater danger to a free people than the escape of some criminals from punishment." *United States v. De Ri*, 332 U.S. 581, 595 (1948).

In this case, FICOR has applied a foreign intelligence exception that this Court has declined to recognize. In fact it has done so in the face of the logic and holding of the *Keith Case*. FICOR's holding is also problematic because it fails to delineate what is being excepted from. Pre-FISA cases generally treat the supposed Foreign Intelligence exception as a deviation from the warrant requirement, as opposed to the requirement of an individualized quantum of suspicion such as probable cause. *Cf. In Re: Certified Questions*, slip op. 16-01 (FICOR 2016) ("We conclude that…the incidental collection of content information during the collection of post-cut-through digit…is constitutionally reasonable, even when done without a probable-cause warrant.").

FICOR's whole purpose is to serve as the neutral and detached magistrate imposed to restrain the Executive's role. FICOR and FISC find their genesis in the suggestion of the *Keith* court that Congress designate a special court to hear and determine national security wiretap applications. *Keith*, 407 U.S. at 323. Here the FICOR has essentially abdicated its function by allowing the Government to collect constitutionally protected content information, without the constitutional safeguards.

A. The Pen Register Statutes

There are two Register Statutes, one in Title 18 applying to domestic cases and the other within the

FISA statute. 18 U.S.C. § 3121 *et seq.*; 50 U.S.C. § 1841 *et seq.* The two statutes cross reference each other and are defined to specifically exclude content. Pen Registers are supposed to intercept "dialing" "routing" "addressing" and "signaling" information ("DRAS"). 18 USC 3127(3),(4); 50 USC 1841(2). In more general terms, Pen Registers are normally combined with Trap & Trace devices to capture and record all incoming or outgoing phone numbers dialed. The terminology itself comes from practice in the 1960's when the modern Public Switched Telephone Network was laid out. In that time period a Pen register was a mechanical counter, a little bigger than a pen, which would dimple onto a string of register tape the dialed phone numbers. In contrast a Trap & Trace device was normally a diode based device which would prevent the mechanical hang up signal from being transmitted until an operator had time to trace the incoming phone number. Pen Register applications are now normally, and frequently, combined with a Trap & Trace device order, leading Courts to treat them interchangeably.

Pen Registers are constitutionally unregulated. *Smith v. Maryland,* 442 U.S. 735 (1979). The dialing information they intercept, because it is voluntarily given over to the phone company, has no expectation of privacy. *Smith*, at 746. Indeed, keeping track of phone calls in and out is still information that phone companies need in order to properly bill their customers. However, after the 2001 terrorist attacks, the USA PATRIOT Act modified the definition of Pen Registers to include all electronic data. Despite subsequent tinkering in

the Protect America Act and the FISA Amendment Act, Pen Registers are now generally authorized for all electronic signaling—including internet traffic.

After the Watergate scandals involving bugging and widespread abuses of the intelligence agencies detailed in the Rockefeller Commission Report and the Church Committee, Congress decided to regulate Pen Registers. The Omnibus Crime Control Act of 1968 (Title III) did not regulate Pen Registers but rather "interception[s]" and proper wiretaps. In light of the *Smith* casp, Congress required that the Government present a judge with an application before installing a Pen Register.

This mandatory nature of Pen Register applications is what makes them different from a Search Warrant. Judicial supervision in the Pen Register context is not constitutionally required, simply being an act of congressional grace. Because Pen Registers, by definition, exclude all content information there is nothing constitutionally protected, and no violation of rights can occur. In similar vein because DRAS data is not constitutionally protected, it "does not require a showing of probable cause to authorize pen register interceptions." *In Re: Certified Questions*, at 36 (App. At 77).

B. The *Ratio Decendi* of the Decision Below

There are two critical assumptions in the FICOR decision. First is that the collection of constitutionally protected content information, without a search warrant, is acceptable so long as

it is "incidental." The second is that the (alleged) lack of technology to sort content from non-content information is sufficient reason to allow the collection of all information.

For the first time, and essentially against the universal opinion of other Federal Courts, and the weight of history, the FICOR decision deliberately allows the Government to invade constitutionally protected information without safeguard or restriction. No showing of suspicion or probable cause required. The FICOR decision characterizes the collection of content information as "incidental" to the collection of non-content information. It cannot properly be characterized as "incidental" when the Government has actual knowledge that some, or most, of the PCD information it is collecting is protected.

The FICOR decision condones the collection of constitutionally protected content information without a Search Warrant, under the guise of the Pen Register scheme which requires no showing of suspicions or probable cause. Probable Cause is a flexible standard designed to give "fair leeway for enforcing laws" and "seek to safeguard citizens from rash and unreasonable interferences with privacy." *Brinegar v. United States*, 338 U.S. 160, 176 (1949).

> The rule of probable cause is a practical, nontechnical conception affording the best compromise that has been found for accommodating these often opposing interests. Requiring

> more would unduly hamper law enforcement. To allow less would be to leave law-abiding citizens at the mercy of the officers' whim or caprice.

Brinegar, 338 U.S. at 176. Although the court below harped upon the "textual command" of reasonableness, probable cause and search warrants are also textual guarantees of the Fourth Amendment. *Cf. In Re: Certified Questions*, slip op. 16-01 at 26 (FICOR 2016) ("[W]hen it comes to intrusions of this kind, the warrant requirement is sometimes a poor proxy for the textual command of reasonableness." (App. At 65).). Relying on the premise that "the ultimate touchstone of the Fourth Amendment is reasonableness" FICOR dispensed with both the warrant requirement and the probable cause requirement. *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006) (quotations omitted). However this is "a line of reasoning that abstracts from the right to its purposes, and then eliminates the right." *United States v. Gozalez-Lopez*, 548 U.S. 140, 145 (2006) (quotation marks omitted) *quoting Maryland v. Craig*, 497 U. S. 836, 862 (1990) (Scalia, J., dissenting). Speaking of the Sixth Amendment right to counsel, the Court said "[The Constitution] commands, not that a trial be fair, but that a particular guarantee of fairness be provided." *Gonzalez-Lopez*, 548 U.S. at 146. Likewise, the Fourth Amendment provides particular textual guarantees of judicial review of a search warrant based on probable cause. These particular textual procedures are not to be disregarded lightly, or without appropriate substitute. *Boumediene v. Bush*, 128 S. Ct. 2229,

2266 (2008) (characterizing necessary requirements of adequate *habeas corpus* substitute).

C. Content - non content Distinction

The Pen Register Statutes, both of them, distinguish between content and non-content information. The statutes, which are cross referenced, are targeted at dialing, routing, addressing, and signaling information ("DRAS"). The Pen Register Statutes were written with constitutional underpinnings. The Content - non content distinction is "a line identical to the constitutional distinction" as that "drawn by the… Supreme Court in *Smith v. Maryland*, 442 U.S. 735, 741-43 (1979)," H.R. Rep. No. 107-236(I), at 53.

The distinction between content and other information, giving rise to an expectation of privacy, is older than the modern history of the Fourth Amendment. *Ex Parte Jackson*, 96 U.S. 727 (1877) (holding that the Fourth and First Amendment apply to the transmission of mail).

> The difficulty attending the subject arises, not from the want of power in Congress to prescribe regulations as to what shall constitute mail matter, but from the necessity of enforcing them consistently with rights reserved to the people, of far greater importance than the transportation of the mail. In their enforcement, a distinction is to be made between

different kinds of mail matter, — between what is intended to be kept free from inspection, such as letters, and sealed packages subject to letter postage; and what is open to inspection, such as newspapers, magazines, pamphlets, and other printed matter, purposely left in a condition to be examined. Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles. The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household. No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and all regulations adopted as to mail matter of this kind must be

> in subordination to the great principle embodied in the fourth amendment of the Constitution.

Ex Parte Jackson, 96 U.S. at 732-733. This holding predates the exclusionary rule and incorporation of the Fourth Amendment, to apply against the states. The Government's position stands against this age-old holding, and the constitutionally-informed express prohibitions in the Pen Register Statutes upon invading content. The FICOR's decision stands alone against a cavalcade of other federal courts which have prohibited the collection of any PCD because it might include content. In fact the FISC noticed in its original certification of the issue to FICOR, that "every other court" to consider the issue of post-cut through digit collection has substantially prohibited any such collection.

Most importantly, the content-non content distinction laid out by *Ex parte Jackson* was seized upon by the Court in *Smith v. Maryland* as the constitutional justification for excluding Pen Registers from the reach of the Fourth Amendment. *Smith*, 442 U.S. at 741 ("Yet a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the contents of communications."). It is sophistry of the rankest kind to claim *Smith* as justification for the constitutional reasonableness for the use of pen registers, but then deliberate undermine its holding by allowing access to content without a warrant or probable cause. Lower courts have been jealous in guarding the privacy right of American

citizens and the core of the Fourth Amendment. A leading case dealing with advancing technology, and the Government's attempts to reach protected information through back-door legal processes which do not conform to the probable cause and warrant requirements is *United States v. Warshak*. *Warshak*, 631 F.3d 266 (6th Cir. 2010) (holding that Stored Communications Act was unconstitutional under the Fourth Amendment because it granted the Government the right to subpoena, without warrant or probable cause, private emails).

The FICOR decision is novel and against the weight of this Court's jurisprudence. The FICOR decision also holds against the vast of weight of authority of almost every other Federal Court that has considered the issue of PCD data. This Court ought to grant review.

2. The Decision below has wide public policy import--Statutory Interpretation

Leaving aside the weighty constitutional concerns, the FICOR decision is indefensible in terms of statutory construction. The Communications Assistance to Law Enforcement Agencies Act (CALEA) allows the Government to require the surreptitious assistance of telephone companies, upon a public utility theory, covering both technical expertise and equipment. Currently the Pen Register statutes require the Government to use "all reasonably available technology" to aid it in avoiding the interception of constitutionally protect content information. The primary thrust of the FICOR decision turns upon the lack of reasonable

available technology to sort out content from non-content.

For reasons laid out above, the FICOR decision breaks the time-honored rule of constitutional avoidance. As a rule of statutory construction, the constitutional avoidance doctrine assumes that Congress knew what it was doing when the statute was written and therefore requires all statutory doubts to be directed away from constitutional questions. The doctrine also requires that, where possible, a statute be interpreted in a manner to ensure its constitutional validity. Here the FICOR simply assumed, without much explication, the availability and application of a "foreign intelligence exception." The FICOR decision expressly allows for the exception of content information upon a pen register application.

The FICOR decision is also faulty for failing to apply the plain meaning rule. A straight textual reading of the Pen Register statutes exclude content by definition. 50 U.S.C. § 1841. The "reasonably available" technology provision is a savings clause of the same type interpreted in *Keith*. The result here must be the same as *Keith*. A savings clause may be directed at unimaginable or largely inconceivable directions. However a savings clause does not convey authorization to perform an activity. The same rule held in *Keith,* that a savings clause protecting any existing inherent constitutional power that the President had to wiretap in the name of national security, did not convey an unrestricted power to wiretap in the name of national security.

Even on its own terms, the FICOR decision is poorly considered on a record without much fact-finding. Solely upon the Government's representations that sorting content from non-content dialed digits was not technologically feasible, FICOR rested its decision. Attorney Zwillinger, the *amicus* below, contested the Government's technological representations.

Some context for that decision is appropriate. Decisions under the FISA statute are implemented by the Nation's intelligence agencies, primarily the National Security Agency. The National Security Agency, and other intelligence agencies, receive a largely secret budget which collectively amounts to approximately $52.7B. The intelligence agencies, properly, have tens of thousands of people who work for them. They have statutory authorization to run special schools and scholarship programs to assist in recruiting talent in highly sensitive fields and technologies. The military and intelligence agencies regularly engage in boundary breaking research, including the development of the internet itself through the Defense Advanced Research Projects Agency ("DARPA"). The technology which is not "reasonably available" to such a behemoth agency with such statutory freedom, amazing manpower, and incredible resources must be well nigh impossible.

The FICOR was very dismissive and hostile to Attorney Zwillinger's approach to simply terminate phone digit collection at 10 dialed digits. FICOR conceded that such an approach would exclude all

content information, but it would also exclude all Post-cut through digits including some information that the Government might be entitled too. Because the Government might not get all that it is allowed to have, specifically constitutionally unregulated information, FICOR decided to allow the Government to deliberately pierce protected information.

It might be true that if the Government narrows the analogy to a speciously small technical problem, it might be impossible to distinguish protected content information from non-content unprotected envelope information. However that does not justify turning constitutional or statutory paradigm on its head. The Government requires justification to invade the protected constitutional sphere. The fact that the Government cannot distinguish the information is not sufficient to allow the invasion of the constitutional sphere, but should deny access to all indistinguishable information until probable cause is shown and a search warrant is obtained.

As an example the undersigned *amicus* undertook to develop a unique computer program, hand-crafted just for this case. The *Amicus* developed and tested a computer program to sort out some forms of protected information. The expert report and actual computer code is included within the addendum of the brief. The program is capable of sorting out and discarding fax signals, audio, speech, and all non-telephone digit data, in real time. Any non-conforming data is immediately discarded. No human ear or eye will see or hear

protected information, simply from a program developed from scratch on a hobbyist basis by interested amicus.

Post PATRIOT ACT, the Pen Register statutes now cover all electronic routing data, including SMS text messages, dialed digits, fax machine signals, internet web traffic, email routing information, cell tower routing data, and all kinds of signals. This Court has already noted that reasonable expectations of privacy may change in light of the new technological era. *United States v. Jones*, 132 S. Ct. 945, 962 (2012) (Alito, J. concurring). Many academic commentators have attacked the third-party doctrine of *Smith v. Maryland* as no longer constitutionally feasible in the current world.

Even on the exact question of post-cut through dialed digits, the Federal Courts have almost universally declined to allow the Government to access the information solely upon the no-showing, no-suspicion, no-warrant basis of the Pen Register statutes.

There are other means to allow the Government to obtain the information it seeks, without a dragnet of protected data in a pen register scheme designed not to include content. For example the Government's primary fear is that it if doesn't have access to post-cut through dialed digits, it might be possible to call a long distance phone service or an operator and have a call routed through to another party. It would be terribly easy to assemble a database of companies with the capability to re-route phone calls and track outgoing phone

numbers, and then compare the time of the calls with the time the suspect called the operator. If MCI or the ATT operator made an outgoing call within 2 minutes of a terror suspect dialing the operator, it is easy to make the inference of who the real party in interest for the phone call is.

Another easy way of sorting out protected content information would be a timing requirement on the dialed digits. Most humans dial phone digits in predictable groups. Assumptions such as this are actually built into the structure of the telephone network. Credit card numbers which are protected information, are normally dialed in 4x4 groups where phone numbers follow the predictable 3-3-4 groups. Another clever limitation would exclude any string longer than the 10 digits required to dial a phone number. Although more complex, the international standardization of phone numbers would allow the Government to make similar assumptions about international telephone calls.

There is no shortage of reasonable steps the government could take to avoid hoovering up all dialed digits, including content, and saving them for analysis later. The savings clause was actually intended to put an extra duty upon the government to avoid impinging upon constitutional protected content. However, FICOR turned the statute on its head by allowing the Government to access constitutionally protected information, without the required constitutional safeguards, simply for the Government's convenience. The fact that the Government might not be allowed to get unregulated information which it is allowed, but

not required, to access is not reason to allow it access to information that it cannot otherwise get. To follow the analogy back to its roots in *Ex Parte Jackson*, there mere fact that someone might mail a package containing a 2nd letter to be re-mailed later does not justify breaking the seal and accessing the contents of the first package. Nor could the Government invade a house, a protected space, simply because there might be information in it that the Government is entitled to. Nor may the Government place a GPS on a car for long-term surveillance simply because it might have been possible to secrete a tiny coachman in a carriage. The Government's convenience, or its claimed right to access some information, is not the guiding light of the constitution which is founded on liberty. The Government, which is capable of being an amazing instrument of oppression, is deliberately shackled to specific constitutional guarantees and procedures to inconvenience it to produce freedom for the populace. "The F[ourth] Amendment itself reflects a judgment by the American people that the benefits of its restrictions on the Government outweigh the costs." *United States v. Stevens*, 130 S.Ct. 1577, 1585 (2010).

"[T]his Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end." *Keith*, 407 U.S. at 317 (quotation omitted). "[T]he F[ourth] Amendment protects against the Government; it does not leave us at the mercy of *noblesse oblige*. We would not uphold an unconstitutional statute

merely because the Government promised to use it responsibly." *United States v. Stevens*, 130 S.Ct. 1577, 1591 (2010).

The proper interpretation of the Pen Register statutes are significant for public policy reasons. Due to the wide reach of the Pen Register statutes, including all electronic routing information and web traffic, a constitutional use of the procedures is important. It was once widely assumed that the simple impossibility of a widespread dragnet of surveillance against U.S. citizens was enough to protect citizens against a clear threat to liberty and a free society

> That "domestic security" is said to be involved here does not draw this case outside the mainstream of Fourth Amendment law. Rather, the recurring desire of reigning officials to employ dragnet techniques to intimidate their critics lies at the core of that prohibition. For it was such excesses as the use of general warrants and the writs of assistance that led to the ratification of the Fourth Amendment.

Keith, 407 U.S. at 327 (Douglas, J. concurring). The Fourth Amendment expresses "the reassurance [] generally that indiscriminate wiretapping and bugging of law-abiding citizens cannot occur." *Keith* 407 U.S. at 321.

Here the Government offers a promise to collect, but not read Pen Register data without further

authorization. That has recently been codified into the statute. 50 U.S.C. § 1845. In the first place, constitutional rights ought never be subject to the Government's promise of good behavior. Simple observations about human behavior confirm the nursery school adage that a fox's promise to guard the henhouse can never be trusted.

Secondly, the Government will have already inflicted at least some harm to Fourth Amendment guarantees by collecting the information and then storing it. It is precisely for that reason that the Court in *Keith* rejected another governmental promise of responsible behavior, because post-surveillance judicial review would not guard against excess surveillance for cases never brought to trial. "Indeed, post-surveillance review would never reach the surveillances which failed to result in prosecutions. Prior review by a neutral and detached magistrate is the time-tested means of effectuating Fourth Amendment rights." *Keith*, 407 U.S. at 318. The *Keith* case specifically rejected deviation from the warrant requirement and prior judicial authorization because it would allow the Government to invade a constitutional protected sphere unreviewed.

3. The Decision below speaks to the constitutional guarantees of liberty gravely impacting much of American life.

With modern technology, non-content envelope information can provide a very deep view into an average person's life. Remembering the original

purpose of *Jackson* and *Katz* which allowed the distinction to protect privacy, a number of academic commentators have suggested revisiting the distinction and overhauling it in favor of something more protective of privacy. After all, "the Fourth Amendment protects people, not places." *Katz v. United States*, 389 U.S. 347, 351 (1967)

The most demonstrative example of addressing and routing information providing real clues to content is in the arena of internet traffic. Internet traffic, now included within the reach of the Pen Register statute, contains Uniform Resource Locators ("URLs") which are commonly called website addresses. While going to "www.google.com" might not reveal much about a person, "www.aclu.org" or a visit to the Federal Society's website, "www.fed-soc.org" can provide insight into a person. Even phone numbers, when combined with a phone book, can show a person is a bachelor if they phone the local pizza parlor more than three nights a week, or that they are needy if they phone a psychiatrist regularly. Much as Justice Sotomayor said about GPS tracking, Pen Register data may "reflect[] a wealth of detail about [someone's] familial, political, professional, religious, and sexual associations." *US v. Jones,* at 955 (Sotomayor, J. Concurring).

In fact, non-content information can be so specific as to breach attorney client privilege, and the work product privilege. While this Court's website is appropriate encrypted, the FISC and FICOR websites are not. A visit to an address labeled "http://www.fisc.uscourts.gov/public-filings/misc-

16-01-motion-aclu-release-court-records" would show that someone was following another controversy presently before the FISC. One could easily surmise that an advocate was preparing to make a fundamental argument about justice and the power of the courts to provide remedies for errors, if the advocate visited, "http://scholar.google.com/scholar_case?case=9834052745083343188&q=marbury+v.+madison&hl=en&as_sdt=40006." Now that the Government may collect advanced knowledge of Attorney Work Product, without even a Search Warrant, the gut of the Sixth Amendment may be undermined. In like vein, the concerns expressed by Justice Douglas about surveillance undermining and eventually extinguishing First Amendment freedoms through chilling and suppressing expression and dissent remain poignant. *Keith*, at 330-333 (Douglas, J. Concurring). Combined with the fact that Pen Register information can be cheaply stored and accessed years later, a horrifying ability to track someone's life and thought process emerges. *United States v. Jones*, at 955-956 (Sotomayor, J.).

In light of the increasingly revealing nature of non-content information, this Court may, in the near future, need to revisit the distinction in order to keep the Fourth Amendment, and other Amendments, alive as a guarantee of liberty. For today, these concerns are simply consequences that will occur if the FICOR decision stands, especially given that it is one of a few courts, like this one, that have immediate nationwide effect.

a. The 2nd Prong of *Katz*

Even though this Court made clear in *United States v. Jones* that the traditional common-law trespass analysis was still alive under the Fourth Amendment, the rubric provided by Justice Harlan's concurrence in *Katz v. United States*, 389 U.S. 347 (1967) is the primary guarantee of constitutional privacy. That rubric, focusing on "people[] not places," looks for a reasonable expectation of privacy and a societal willingness to protect it. *Katz,* at 361.

The "societal willingness to protect" prong is important in the context of evolving technology. Both the dissent and the concurrence in *Jones* acknowledged that new technologies may require the Court to reframe the constitutional guarantee.

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.… This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the

> books, groceries, and medications they purchase to online retailers… I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year.

US v. Jones, at 957 (Sotomayor, J. Concurring). The "reasonably available" technology language is an extra duty upon the Government to consciously and scrupulously avoid constitutionally protected content information. Society has now reached a maturity point where such a duty can and should be imposed within the *Katz* formulation as a constitutional obligation.

b. An exemplar

The *Amicus's* computer program provides an excellent example of the technological possibilities for privacy protection. Tested with over 400 years of audio signals, the program can in real time sort out all voice and fax or computer signals, leaving only digital dialed touch-tone phone signals. The program has a high success rate.

While new technology allows the Government to do amazing things, perhaps approaching an Orwellian reality, the technology also allows for a close supervision of the Government. Now, more than ever before, remedies can be narrowly tailored. While the founding generation winced at the Government viewing papers, we have since created

remedies to allow the Government to seize and review entire filing cabinets with "taint teams," and have applied that theory to computer records. *United States v. Tamura*, 694 F.2d 591 (9th Cir.1982); *Unites States v. Comprehensive Drug Testing Inc*, 621 F.3d 1162 (9th Cir. 2010). Computer programs like the one generated for this Court by the *Amicus* can and should become standard in dealing with Government searches of large swaths of information. The Fourth Amendment places, upon the Government, the burden to justify an intrusion into the constitutionally protected private sphere.

More over the particularly requirement, all to easily ignored in a digital world, is a "textual command" that the Governmental intrusion be controlled and limited. Vague executive guidelines about minimization are plainly insufficient when compared to the guarantee of advance judicial review. *Keith*. The Court should strongly consider not merely respecting the constitutional right, but imposing an affirmative duty upon the Government going forward.

A program such as the one submitted here is inexpensive to develop and very resource efficient. The *Amicus* tested the ability of the program to run against an audio stream in real time and the test was successful. The program is a discriminator, which prevents the Government from ever coming into possession of protect information by discarding that which the Government is not allowed to possess. Such a process contains much less risk of Government malfeasance than simply storing

information for later, under a dubious promise that the Government will not make further use of it without authorization.

A real-time limiter such as the program here also avoids running afoul of the Fourth Amendment issues inherent in storing information for later analysis. *Keith* and other cases make clear that unauthorized surveillance itself is a Fourth Amendment violation. Storing the information, to sort out what is permissible and what is not permissible at a later date is still a violation for the interception of data the Government was never entitled to in the first place. Despite the Government's policy arguments, the Government always bears the burden to justify the intrusion. Absent a search warrant, founded on probable cause, particularized to a specific subject, with a controlled scope of search, the constitutional protections of privacy are a dead letter.

4. The Decision implicates the balance between liberty and national security

The FICOR decision draws a great deal of intellectual weight from the assertions of national security and concerns about terrorist attacks. While these are weighty concerns, they cannot justify abandoning the guarantees of freedom contained within our Bill of Rights. Time and again, this Court has emphasized that our Constitution endures in peace and in war.

> Even the war power does not remove constitutional limitations safeguarding essential liberties… this concept of

> "national defense" cannot be deemed an end in itself, justifying any exercise of legislative power designed to promote such a goal. Implicit in the term "national defense" is the notion of defending those values and ideals which set this Nation apart. For almost two centuries, our country has taken singular pride in the democratic ideals enshrined in its Constitution… It would indeed be ironic if, in the name of national defense, we would sanction the subversion of one of those liberties—the freedom [from unreasonable search and seizure]—which makes the defense of the Nation worthwhile.

United States v. Robel, 389 U.S. 258, 264 (1967).

Conclusion

Wherefore the Amicus respectfully pray that this Honorable Court grant the petition for certiorari and hear the case.

Respectfully Submitted

/S/ John Walsh
Counsel of Record
Walsh & Walsh LLP
PO Box 9
Lynnfield, MA 01940
617-257-5496

Appendix

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

~~SECRET//ORCON/NOFORN~~

United States Foreign Intelligence
Surveillance Court of Review

IN RE: CERTIFIED QUESTIONS OF LAW

Docket No. FISCR 16-01

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

Decided:

Marc Zwillinger, ZwilGen 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 Stated. 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 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 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]

[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.

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 government "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]

[2] The statute that defines pen registers and trap-and-trace devices for the purposes of this case

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 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

---

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."

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.

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

---

[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"—*id.* 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.

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 Text]. 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 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 tit1e 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

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

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 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:

> [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

[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

post-cut-through content information, it is impossible to know in advance 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. 2007); *In re Application of the United States,* 441 F. Supp. 2d 816 (S.D. Tex. 2006).[6]

---

[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

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 government 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

---

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).

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 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 "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 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 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]

---

[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 uploading documents, and

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 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.

---

drafting emails. [Redacted Text]. 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.

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 insta11ed 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).

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.

---

[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).

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 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

[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

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.

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

---

interception will inevitably occur, but that the agency must take steps to keep that interception to a minimum.

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 312l(c) to cover technologies other than telephony. *Id.*
§ 216(a).

Second, Congress modified section 312l(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 "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 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 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*

u. United States, 490 F.3d 455 (6th Cir. 2007), *vacated,* 532 F.3d 521 (6th Cir. 2008) (en bane). 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 (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 digit—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 modem 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).

Five years later, in *United States u. 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 u. 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 bane); *United States v. Brown,* 484 F.2d 418, 426 (5th Cir. 1973). *But see Zweibon u. Mitchell,* 516 F.2d 594, 633-51 (D.C. Cir. 1975)

(en bane) (plurality opinion) (suggesting, in dictum, that no such exception exists).[10]

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

---

[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 □□□□try," 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. 1983); *Chagnon u. Bell,* 642 F.2d 1248, 1259 (D.C. Cir. 1980).

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 Warrant 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

[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.

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

[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 purpose." *Id.* We therefore concluded that the more sensible requirement was that the "programmatic purpose" of the intelligence-gathering "involve[]

the government were constrained 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

---

some legitimate objective beyond ordinary crime control." *Id.*

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 legitimate 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 supervision 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 riot render those acquisitions unlawful.")).

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 prohibition on use protects

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

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

---

never even sought such an order. See also Record on Appeal, Certification at 2 n.l.

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 connection 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 u. 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.ll ("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).

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 employed 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

---

[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).

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 making 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.

Statutory Provisions

28 U.S.C. § 1254
Cases in the courts of appeals may be reviewed by the Supreme Court by the following methods:
(1)By writ of certiorari granted upon the petition of any party to any civil or criminal case, before or after rendition of judgment or decree;
(2)By certification at any time by a court of appeals of any question of law in any civil or criminal case as to which instructions are desired, and upon such certification the Supreme Court may give binding instructions or require the entire record to be sent up for decision of the entire matter in controversy.

50 U.S.C. § 1803

(b) Court of review; record, transmittal to Supreme Court
The Chief Justice shall publicly designate three judges, one of whom shall be publicly designated as the presiding judge, from the United States district courts or courts of appeals who together shall comprise a court of review which shall have

jurisdiction to review the denial of any application made under this chapter. If such court determines that the application was properly denied, the court shall immediately provide for the record a written statement of each reason for its decision and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

(f))Stay of order
(1)A judge of the court established under subsection (a), the court established under subsection (b) or a judge of that court, or the Supreme Court of the United States or a justice of that court, may, in accordance with the rules of their respective courts, enter a stay of an order or an order modifying an order of the court established under subsection (a) or the court established under subsection (b) entered under any subchapter of this chapter, while the court established under subsection (a) conducts a rehearing, while an appeal is pending to the court established under subsection (b), or while a petition of certiorari is pending in the Supreme Court of the United States, or during the pendency of any review by that court.
(2)The authority described in paragraph (1) shall apply to an order entered under any provision of this chapter.

(k)Review of FISA court of review decisions
(1)Certification
For purposes of section 1254(2) of title 28, the court of review established under subsection (b) shall be considered to be a court of appeals.

(2)Amicus curiae briefing
Upon certification of an application under paragraph (1), the Supreme Court of the United States may appoint an amicus curiae designated under subsection (i)(1), or any other person, to provide briefing or other assistance.

50 U.S.C. § 1861(f)(3)

(3) A petition for review of a decision under paragraph (2) to affirm, modify, or set aside an order by the Government or any person receiving such order shall be made to the court of review established under section 1803(b) of this title, which shall have jurisdiction to consider such petitions. The court of review shall provide for the record a written statement of the reasons for its decision and, on petition by the Government or any person receiving such order for writ of certiorari, the record shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

50 U.S.C. § 1881a(h)(6)(B)

(B)Certiorari to the Supreme Court
The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

50 U.S.C. § 1881a(i)(4)(D)

(D)Certiorari to the Supreme Court
The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

18 U.S.C. § 3121

(a)In General.—
Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).
(b)Exception.—The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service—
(1)relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or
(2)to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from

fraudulent, unlawful or abusive use of service; or (3) where the consent of the user of that service has been obtained.
(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.
(d)Penalty.—
Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

18 U.S.C. § 3127(3),(4)

(3)the term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire

communication service for cost accounting or other like purposes in the ordinary course of its business; (4)the 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;

50 U.S.C. § 1841

As used in this subchapter:
(1)The terms "foreign power", "agent of a foreign power", "international terrorism", "foreign intelligence information", "Attorney General", "United States person", "United States", "person", and "State" shall have the same meanings as in section 1801 of this title.
(2)The terms "pen register" and "trap and trace device" have the meanings given such terms in section 3127 of title 18.
(3)The term "aggrieved person" means any person—
(A)whose telephone line was subject to the installation or use of a pen register or trap and trace device authorized by this subchapter; or
(B)whose communication instrument or device was subject to the use of a pen register or trap and trace device authorized by this subchapter to capture incoming electronic or other communications impulses.
(4)
(A)The term "specific selection term"—

(i)is a term that specifically identifies a person, account, address, or personal device, or any other specific identifier; and
(ii)is 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.
(B)A specific selection term under subparagraph (A) does not include an identifier that does not 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, such as an identifier that—
(i)identifies an electronic communication service provider (as that term is defined in section 1881 of this title) or a provider of remote computing service (as that term is defined in section 2711 of title 18), when not used as part of a specific identifier as described in subparagraph (A), unless the provider is itself a subject of an authorized investigation for which the specific selection term is used as the basis for the use; or
(ii)identifies a broad geographic region, including the United States, a city, a county, a State, a zip code, or an area code, when not used as part of a specific identifier as described in subparagraph (A).
(C)For purposes of subparagraph (A), the term "address" means a physical address or electronic address, such as an electronic mail address or temporarily assigned network address (including an Internet protocol address).
(D)Nothing in this paragraph shall be construed to preclude the use of multiple terms or identifiers to meet the requirements of subparagraph (A).

18 U.S.C. § 1845

(a)In general
(1)Information acquired from the use of a pen register or trap and trace device installed pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the provisions of this section.
(2)No information acquired from a pen register or trap and trace device installed and used pursuant to this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.
(b)Disclosure for law enforcement purposes
No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.
(c)Notification of intended disclosure by United States
Whenever the United States intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States against an aggrieved person any information obtained or derived from the use of a pen register or trap and trace device pursuant to this subchapter, the United States shall, before the trial, hearing, or the other proceeding or at a reasonable time before an

effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the United States intends to so disclose or so use such information.

(d)Notification of intended disclosure by State or political subdivision

Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the State or political subdivision thereof against an aggrieved person any information obtained or derived from the use of a pen register or trap and trace device pursuant to this subchapter, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(e)Motion to suppress

(1)Any aggrieved person against whom evidence obtained or derived from the use of a pen register or trap and trace device is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, or a State or political subdivision thereof, may move to suppress the evidence obtained or derived from the use of the pen register or trap and trace device, as the case may be, on the grounds that—

(A)the information was unlawfully acquired; or
(B)the use of the pen register or trap and trace device, as the case may be, was not made in conformity with an order of authorization or approval under this subchapter.
(2)A motion under paragraph (1) shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the aggrieved person concerned was not aware of the grounds of the motion.
(f)In camera and ex parte review
(1)Whenever a court or other authority is notified pursuant to subsection (c) or (d), whenever a motion is made pursuant to subsection (e), or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to the use of a pen register or trap and trace device authorized by this subchapter or to discover, obtain, or suppress evidence or information obtained or derived from the use of a pen register or trap and trace device authorized by this subchapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority shall, notwithstanding any other provision of law and if the Attorney General files an affidavit under oath that disclosure or any adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the use of the pen register or trap and trace device, as the case may be, as may

be necessary to determine whether the use of the pen register or trap and trace device, as the case may be, was lawfully authorized and conducted.
(2)In making a determination under paragraph (1), the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the use of the pen register or trap and trace device, as the case may be, or may require the Attorney General to provide to the aggrieved person a summary of such materials, only where such disclosure is necessary to make an accurate determination of the legality of the use of the pen register or trap and trace device, as the case may be.
(g)Effect of determination of lawfulness
(1)If the United States district court determines pursuant to subsection (f) that the use of a pen register or trap and trace device was not lawfully authorized or conducted, the court may, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from the use of the pen register or trap and trace device, as the case may be, or otherwise grant the motion of the aggrieved person.
(2)If the court determines that the use of the pen register or trap and trace device, as the case may be, was lawfully authorized or conducted, it may deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.
(h)Binding final orders
Orders granting motions or requests under subsection (g), decisions under this section that the use of a pen register or trap and trace device was

not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to the installation and use of a pen register or trap and trace device shall be final orders and binding upon all courts of the United States and the several States except a United States Court of Appeals or the Supreme Court.

CCAD: the Call Contents Automatic Differentiator

Introduction

In this paper, we describe CCAD, the Call Contents Automatic Differentiator, a naive system for extracting post-cut-through dialing digits while excluding post-cut-through content digits. The system runs with an expected accuracy of 99.4 percent and 98.3 percent in the worst case. Such a system is critical in differentiating so-called "envelope information" (which may legally be collected without a warrant) from "content information" (which may not). This paper describes the algorithm used. Though the specific algorithm is unique, it combines well understood algorithms in an intuitive manner.

We will first discuss the history and technology of the telephone. Then we will detail assumptions made about the audio input to the algorithm and detail the algorithm itself, followed by a description of test methodology. Next, we discuss the results and possible improvements to the algorithm, were it to be deployed in a real-world environment. Finally, we conclude with a summary of findings.

Background

In modern society, we often dial telephones but rarely think about what is required to connect a

telephone call. This section explores this topic, as well as some telephonic and digital signals processing (DSP) history.

To start at the highest level, the network used to connect one telecommunications user to another is the PSTN (Public Switched Telephone Network). The first deployment of what would eventually become the PTSN was Bell Telephone Company's, in 1878 [Gast 2001]. Dialing methods have evolved and adapted as the network has grown and as technology has advanced. Initially, operators were required to connect every call - manually plugging short lengths of cable to connect different "circuits" (essentially creating a point to point telephone line). Later, rotary dialing was introduced as a way to automate dialing and reduce the number of operators required. In 1960, the first paper on DTMF (Dual-Tone Multi-Frequency) dialing was published in the Bell System Technical Journal [Schenker 1960]. The first introduction of DTMF to the PTSN happened on November 18, 1963 [Fox 2013]. With minor variation, DTMF has remained the standard since. Today, the DTMF standards are detailed in the International Telephone Union's recommendations Q.22, Q.23 and Q.24. Recently, much of the phone system has been digitized, but the user-facing interface (DTMF) has remained the same.

DTMF at its core is a set of eight tones (four high and four low) [ITU-T Q.23 1988]. Each pair of tones (one from the high set, one from the low set) conveys one of the signals 0 through 9, A through D, the star and the octothorp ("pound sign"). Though the signals A through D never made it into mainstream use, they remain in the standard.

DTMF decoding software has been around since the origin of Digital Signals Processing (DSP). The oldest freely-available paper on implementing DTMF detection in software we can locate is from 1989 [Mock 1989]. However, we are confident this is not the first software implementation – if nothing else, there would have been proprietary implementations. Paper [Chen 1996] after paper [Clarkson 2004] describing various implementations has followed, as have open-source implementations [Blue 1997][Zapata 2001][Digium 2002].

The algorithm also performs Voice Activation Detection (VAD) – determining which parts of audio contain a person speaking and which contain noise. VAD is an area of ongoing research. However, this paper relies only on one of the many measures used in VAD [Sahidullah 2012] – energy detection. Energy detection simply calculates the average volume of section of speech and is the most obvious and most simple possible measure

for whether or not there is speech in an audio stream. However, it performs extremely poorly if the environment is noisy.

Assumptions

This system makes several reasonable assumptions about the format of a call. First, it assumes that the call it is examining is a user calling an automated system. The canonical example for this software is an international calling service – the user calls in, the service requests subscriber information and the number to be called. Other examples of automated systems include the service lines of banks and other financial institutions. This assumption implies a "call-and-response" style interaction. That is, it assumes that after the call is connected to the initial recipient (callee), information is requested from the caller via a pre-recorded voice prompt (e.g. "Press 1 for English, Press 2 for Spanish...", "Please enter your account number, followed by the pound sign"). The user then responds to this prompt by pressing a button or buttons on their telephone. This process then repeats until the automated service has collected the information it requires.

This system assumes a very minimal PSTN system. It assumes that DTMF is transmitted via the same channel as the voice and would be

audible to any person listening to the call. It also assumes that a single audio stream contains audio from both the caller and the callee. This renders the requirements so simple that this system would work with any relatively modern telephone system, and the technical requirements are met in parts of the US phone system back to the first DTMF deployments and are certainly met by all of the phone system today.

Finally, this system expects that the input audio stream does not begin until after the call has been connected. That is, this assumes it does not receive the originally dialed ten-digit phone number.

The Algorithm

This system uses two-stage process to determine which portions of the audio stream constitute envelope information. Stage 1 is the extraction of a "signal stream" from the audio, containing all DTMF signals and all separators. Stage 2 examines the signal stream using simple heuristic filters to determine what actually is envelope information. The final output of this methodology is any envelope information that was embedded in the audio stream.

Stage 1 of the method extracts DTMF information and timing information from the audio stream.

Timing information is the length of any silences or voice in the audio, and is used to separate DTMF digits into meaningful groups. By default, this implementation considers voice longer than one second or silence longer than ten seconds to constitute a separator between digit groups. In order to do this, we must first differentiate between audio that contains DTMF signals and that which does not. Then, for audio which does not contain DTMF tones, we must discern between voice audio and silence audio.

Extraction of the DTMF signals is a well understood problem. Technical documentation is available going back to the 1980s [Mock 1989] describing (or containing) programs for doing so. The most popular (and simplest to implement) method is the Goertzel Algorithm [Goertzel 1958], which can be used to determine if a specific frequency band is present. Hobbyists have implemented DTMF signal recognition as early as 1997 [Blue 1997] and it is used in leading open-source software [Digium 2002].

The Goertzel Algorithm is applied to the eight DTMF frequencies individually. For each frequency, the output of the Goertzel Algorithm (a unitless magnitude) is compared to a pre-set threshold. If the output is greater than the threshold, the corresponding DTMF frequency

might be present. Next, for every frequency which was greater than the threshold, the first harmonic (frequency twice the original) is checked. DTMF tones are mechanically generated and will not have any output at the first harmonic. In contrast, voice or non-mechanical sounds will have a first harmonic. Therefore, if a first harmonic is detected, the DTMF frequency detection is a false positive and is ignored.

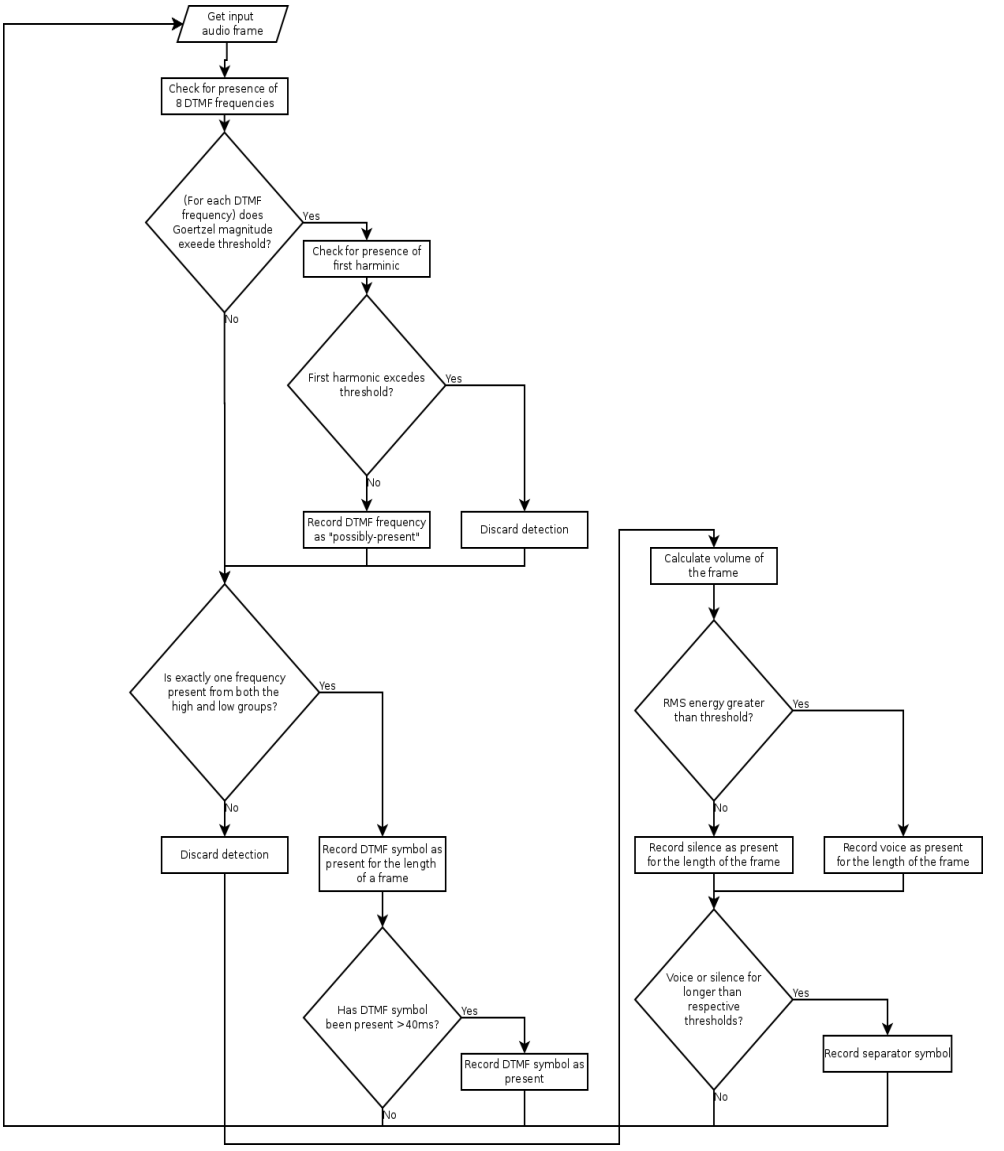
Next, the set of DTMF frequencies detected is examined to make sure that exactly two are present – one from the high set, one from the low. If more than one tone from a set is present, or a set has no tones present, the detection is a false positive and is ignored. If the frequency set passes this test, it is a potential DTMF signal.

Finally, the length of time the DTMF signal has been present is measured. ITU-T Q.23 requires DTMF signals be present for a minimum of 40 milliseconds to be valid, so any shorter signals are ignored. Any potential signal which passes this test is a valid signal and is added to the signal stream.

If a section of audio does not contain DTMF tones, we must then determine if it is silence or voice content. In order to do this, the most naive possible algorithm is used. We simply measure the volume of the section of audio. If it is above a

certain volume, it is voice. If below, silence/noise. The length of each voice and noise section is tracked. If a section of audio contains voice, it is also counted towards the silence length. These lengths are both reset when DTMF signals are detected and the length of voice is reset when silence is detected. If at any point the tracked length of voice goes over one second or the tracked length of silence exceeds ten seconds, a "silence signal" is added to the signal buffer to act as a separator between sequences of DTMF signal

Drawing Logical Flow


Get input audio frame
Check for presence of 8 DTMF frequencies
(For each DTMF frequency) does Goertzel magnitude exeede threshold?
Yes
No
Check for presence of first harminic
First harmonic excedes threshold?
Yes
No
Record DTMF frequency as "possibly-present"
Discard detection
Is exactly one frequency present from both the high and low groups?
Yes
No
Discard detection
Record DTMF symbol as present for the length of a frame
Has DTMF symbol been present >40ms?
Yes
No
Record DTMF symbol as present
Calculate volume of the frame
RMS energy greater than threshold?
Yes
No
Record silence as present for the length of the frame
Record voice as present for the length of the frame
Voice or silence for longer than respective thresholds?
Yes
No
Record separator symbol

In stage two of the algorithm, the DTMF signal buffer is broken into segments. A segment is any series of signals between silence signals. Each segment is then examined for validity as a possible phone number using simple pattern matching. For example, if a sequence of DTMF signals is 10 signals long (or 11 with an octothorp as the final signal) and consists only of zero through nine, it could be a valid US telephone number and is marked as such. On the contrary, a 16-signal DTMF sequence consisting of zero through nine (optionally with the 17th signal as an octothorp), it is not a valid telephone number – more likely a credit card number – and is ignored. As a further example, if a sequence contains A through D, star or an octothorp (with the exception that it may end in an octothorp), it is not a valid telephone number and is ignored.

The implementation accompanying this paper is written to discover domestic (US+Canada) calls only, following the North American Numbering Plan format [NANPA], though it could easily be expanded to include the full range of international numbers defined by the ITU [ITU-T E.164 2011].

Test methodology

CCAD was tested using a modified set of audio from ITU-T Recommendation P.23's supplemental audio database. The “original” (*.SRC) voice files

from this database were preprocessed by removing any sections longer than 0.1 second with a volume less than -40dBFS – in short, by removing any silence – followed by adjusting the volume such that the maximum peak amplitude was 0 dBFS – as loud as possible without losing any content. Only the white noise file from the same database was used to provide noise, and was not modified. The modification of voice files was performed to compensate for the naive VAD algorithm.

Tests were performed in two stages. First, a set of semi-random audio streams was generated. Second, a set of more restricted format audio streams was generated. Each set consisted of 1 million audio streams. For each generated audio stream, the signal stream (DTMF signals and separators based on voice time and silence time) corresponding to the generated audio was saved. The audio stream was run through the detection algorithm implementation and the results compared to the expected results.

The first set of audio streams consist of randomized sequences of DTMF signals, voice samples and noise samples. No ordering between types of audio was imposed. Voice and noise sections had a minimum length of zero and no maximum while DTMF signals were generated in lengths of 1-16, with no restrictions on signal

usage or sequence. This set of input streams was used as a stress test of the DTMF detection and VAD algorithms, determining their accuracy in the worst case. Only the stage 1 output was examined to determine success.

The second set of audio streams was intended to represent more typical inputs. This generated input sequences where a DTMF section was always followed by a voice or silence section exceeding the threshold for separation. This more closely models the call-and-response format assumed by the algorithm under test. Only the stage 2 output was examined to determine success.

In each of these sets of inputs, voice and silence very close (within 100 milliseconds) to their respective time thresholds were shortened or lengthened to be 100 milliseconds to either side of the threshold. This was done to prevent incorrect input files (such as voice input files that contained short silences) from corrupting the test by creating audio sequences which did not match the expected signal sequence.

Performance measurements were gathered on the same machine used to run the million-stream tests. This machine is an Amazon AWS m4.16xlarge machine (64 CPUs, 256 GiB of memory) with an attached 2TiB 20,000 IOPS disk.

Additionally, a second, smaller 10,000 stream test was run on a small system to help determine scaling. The smaller system was a Gigabyte C847N-D motherboard with two Intel Celeron 847 processors (running at 1.10GHz) and 2GiB of memory. When this system was built in 2013, it cost less than $125.

Results

Overall, CCAD showed an excellent success rate, especially for such a naive implementation. The type 1 tests (stress tests) showed a success rate of 98.3 percent, while the type 2 (expected conditions) tests showed a 99.4 percent success rate.

In order to better understand other possible improvements, we conducted an examination of the causes of failure for the first 100 failures in each test type. Failures were categorized as one or more of the algorithm having: missed a DTMF signal, missed a separator signal, added an extra DTMF signal, or added an extra separator. Additionally, failures were marked as either benign or not. A benign failure is only applicable to type 1 tests and represents a failure where the generated signal stream was different, but in which the final output (i.e. detected envelope data) would not be different. This category only captures extra or missing separator signals

adjacent to other separator signals or adjacent to the start or end of the stream.

	Type 1	Type 1 Benign	Type 2
Missed DTMF	0	-	0
Missed Separator	24 (24.3%)	23 (22.8%)	100 (100%)
Extra DTMF	0	-	0
Extra Separator	40 (39.6%)	14 (13.9%)	0

Table 1: Causes of failure

This failure analysis leads to several interesting results. First, about 37 percent of the examined type 1 failures were benign. Each observed benign failure was at the start or the end of the signal stream. Therefore, these are most likely due to differences in accounting in initial or final conditions between the test generator and the implementation than any actual error. If the ratios of failures held for the larger data set and the benign failures were corrected, the type 1 tests would have an accuracy of 98.9 percent – much more in line with the accuracy of the type 2 tests. Second, all of the type 2 failures were due to missing separators.

Finally, it is worth noting that all the failures are due to VAD issues. This indicates that the DTMF detection and the algorithm for identifying valid

phone numbers is extremely robust and reliable. As expected, the VAD algorithm used needs improvement.

It is also worth examining the runtime of these tests to determine what real-world resource usage would be.

	AWS m4.16xlarge	Gigabyte C847N-D
Cores	64	2
Memory (GiB)	256	2
Test size (total type 1&2 streams)	2,000,000	20,000
Test size (total seconds of audio)	245522198.508	2475780.9
Test size (audio, scaled)	466y, 295d, 0:38:30	4y, 258d, 7:00:53
Seconds of audio per core	3836284.3516875	1237890.45
Test runtime (total seconds)	6586.342102	2202.602432
Seconds of audio processed per second per core	582.4605361028	562.0126592142
Minutes of audio processed per second per core	9.7076756017	9.3668776536

Table 2: Performance information

The performance of these two machines – one very

high-end and one very low-end - is surprisingly similar – both were able to process about 570 seconds of audio per second per core.

The average call is about two minutes long [Orlowski 2013] and the average person makes 2.5 phone calls per day [Lenhart 2010]. Let's say we wanted to monitor one million people in the US – about 1/3rd of one percent of the population - an absurdly large percentage to suspect of foreign intelligence or terrorist connections. Assuming no calls between citizens on the watch list, this would mean processing 300,000,000 seconds of audio per day.

Let's first look at Amazon-equivalent systems. This requires about 515,000 Amazon processor cores – just over 8,000 Amazon-equivalent systems. Unfortunately, pricing information is unavailable for hardware equivalent to the Amazon systems.

Next, let's examine what it would take to monitor these calls with the Gigabyte system. It would require about 515,000 processor cores, or about 258,000 systems. Fortunately we do know the pricing information for these systems – the hardware for these systems would cost about $32 million. An exceedingly reasonable price, and one that could be significantly reduced by optimizing the hardware for price per core or by improving

the performance of the CCAD implementation.

While this is a large number of systems, it is by no means unheard of within supercomputing. Further, many of the typical supercomputing problems (power, cooling) can be sidestepped by distributing these systems throughout the country in local telephone exchanges (coincidentally placing them as close to the person being monitored as possible). Data transmission and aggregation would be negligible, given that this system reduces large audio streams (kilobytes or megabytes each) to very small strings of text (bytes each).

In short, monitoring a significant portion of telephone calls made within the US is practicable with the implementation of CCAD accompanying this paper – and would become more practicable with an optimized implementation.

Future Work and Possible Improvements

The list of possible improvements to CCAD is significant. This algorithm is an incredibly naive method for performing this test.

Stage one (signal stream detection) can be massively improved by using more advanced algorithms. This implementation used a simplified Goertzel algorithm simply because it was expedient and easy to find reference material

on.

In this case, the Goertzel algorithm is not very efficient. The Goertzel Algorithm is useful for checking the presence of a single frequency or a small set. However, the algorithm outlined in this paper tests enough frequencies that it is possible that another algorithm from the same family (DFTs – Discrete Fourier Transforms) may be more efficient.

Additionally, the use of the Goertzel algorithm lead to a "windowing" problem. Because the Goertzel algorithm works on finite, non-overlapping sections of audio, the granularity used for timing is extremely coarse – about 10 milliseconds. For the typical DTMF decoder, which is concerned only with determining if and when there are signals present, this is sufficient. For more advanced versions of this algorithm (which need extremely precise timing information, see later in this section) this granularity is so large as to be unusable. Instead, one could substitute an algorithm from the same family which is either non-windowed or uses a sliding window instead.

Any of the algorithms used for audio processing could easily be adapted to run efficiently on GPUs, allowing thousands of streams to be processed simultaneously and extremely efficiently.

Second, the VAD used in this algorithm is incredibly useless outside controlled settings. Instead, a more complete VAD algorithm could be implemented. VAD is an active field of research within DSP (Digital Signals Processing) as it is extremely useful to any application where a speaker may be silent much of the time. Significant research has been devoted to creating and refining various VAD algorithms.

Alternatively, many modern telephone networks have converted to digital transmission of audio. Network providers are able to significantly reduce the infrastructure required by only transmitting when a person is speaking – so they already perform VAD. This is why, for example, when talking on a phone you may only be able to hear some types of background noise when a person is speaking. With the cooperation of a digital telephony network provider, input audio could come "pre-classified" as either silence or non-silence.

Stage two can be improved using various methods to infer intent, rather than simply detecting segments that match the pattern of a phone number. The first and most obvious method is to build a database of known phone numbers. This would store both numbers known not to have envelope information sent via DTMF tones (e.g.:

banks, credit card companies) and those known to have envelope information sent after the initial call is connected (e.g.: international dialing services). Merely through these two categorizations, the great majority of potential envelope information can be properly categorized.

A second potential improvement is to use the "inter-digit time" - the length of time between tones - to guess intent. For example, US phone numbers are written in groups of 3-3-4 (e.g. 555-867-5309). People tend to dial numbers in the same format they're written, with longer pauses between groups of digits. This may be because they're reading them and it is simpler to remember a small part of the number, or because they dial one portion then and then look for the next part or because they've memorized the number in this format. Other numbers of similar lengths will be broken up differently (e.g credit cards – four groups of four), so the pauses between groups of digits will be placed differently.

A third possible improvement is to use voice recognition software to look for keywords or perform language processing to determine if the user is being asked for envelope information.

All of these methods could be combined. When an audio stream first starts, the algorithm would check if the callee's 10-digit number is a known

number stored in the database. Based on this information, it can either ignore the call (if the call will never contain envelope information), or continue listening (if the number is not listed or is known to contain envelope information). If it continues listening, it would then begin transcribing any voice into text and examining it for phrases like “please enter the number you wish to dial”. Concurrently, it would gather precise timing information on the entry of DTMF signals. The presence of keywords and the timing information would be used to weigh whether or not a particular signal sequence likely represents a phone number or not.

Conclusion

In this paper we have described CCAD, the Call Contents Automatic Differentiator, an exceedingly simple and naive system for separating dialed phone numbers, which are routing information, from other data transmitted via the same signaling mechanism (DTMF). We've shown that even such a simple implementation has a worst-case accuracy of 98.3 percent (or 98.9 percent when correcting for certain failures) and an expected accuracy of 99.4 percent. Finally, we have discussed how this system could be improved and deployed for real-world use.

Sources

BLUE, MR. 1997. DTMF Encoding and Decoding In C. Phrack Magazine, 7(50). http://phrack.org/issues/50/13.html

CHEN, CHIOUGUEY J. 1996. Modified Goertzel Algorithm in DTMF Detection Using the TMS320C80. http://www.ti.com/lit/an/spra066/spra066.pdf

CLARKSON, KYLE AND JONES, DOUGLAS L. 2004. Goertzel's Algorithm. http://cnx.org/contents/kw4ccwOo@5/Goertzels-Algorithm

DIGIUM. 2002. dsp.c. http://doxygen.asterisk.org/asterisk1.0/dsp_8c-source.html

FOX, MARGALIT. 8 February, 2013. John E. Karlin, Who Lead the Way to All-Digit Dialing, Dies at 94. New York Times.

GAST, MATTHEW S. 2001. T1: A Survival Guide. O'Reilly, Cambridge, MA.

GOERTZEL, G. 1958. An Algorithm for the Evaluation of Finite Trigonometric Series. The American Mathematical Monthly, 65(1), 34-35. http://www.jstor.org/stable/2310304

ITU-T Recommendation E.164. 2011. The International Public Telecommunications

Numbering Plan. http://www.itu.int/rec/T-REC-E.164/en

ITU-T Recommendation Q.22. 1988. Frequencies to be used for in-band signaling. http://www.itu.int/rec/T-REC-Q.22/en

ITU-T Recommendation Q.23. 1988. Technical Features of Pushbutton Telephone Sets. http://www.itu.int/rec/T-REC-Q.23/en

ITU-T Recommendation Q.24. 1988. Multifrequency push-button signal reception. http://www.itu.int/rec/T-REC-Q.24/en

LENHART, AMANDA. 2 September, 2010. Cell Phones and American adults. http://www.pewinternet.org/2010/09/02/cell-phones-and-american-adults/

MOCK, PAT. 1989. Add DTMF Generation and Decoding to DSP-mP Designs. http://www.ti.com/lit/an/spra168/spra168.pdf

NORTH AMERICAN NUMBERING PLAN ASSOCIATION. (N.D.). NANPA: Numbering Resources – NPA (Area) Codes. https://www.nationalnanpa.com/area_codes/index.html

ORLOWSKI, ANDREW. 30 January 2013. "The Death of Voice: Mobile phone calls now 50 per cent shorter". The Register.

http://www.theregister.co.uk/2013/01/30/mobile_phone_calls_shorter/

SAHIDULLAH, MD AND SAHA, GOUTAM. Comparison of Speech Activity Detection Techniques for Speaker Recognition. https://arxiv.org/pdf/1210.0297.pdf

SCHENKER, L. 1960. Pushbutton Calling with a Two-Group Voice-Frequency Code. The Bell System technical Journal, 39(1).

ZAPATA COMPUTER TELEPHONY TECHNOLOGY. 2001. goertzel.c. https://sourcecodebrowser.com/zapata/1.0.1/goertzel_8c_source.html

CCAD Computer Code (annotated)

```
/*
This module attempts to implement the following pseudocode.  This code extracts
phone numbers (and only valid phone numbers) from audio recordings.  The intent
is to extract only valid routing data from calls without running the risk of
capturing content, both of which could be carried by DTMF tones.  In this way,
it functions as an automated "taint team", extracting data that can be legally
captured without allowing the government undue access to sensitive information
that should not be captured.

It makes the following assumptions:
1. non-DTMF content (voice) can act as the separator between content that is
  permissible to capture and that which isn't.  For example, this could be the
  separation between a user inputting a credit, subscriber or calling card
  number and the number the user is attempting to call
2. There is some amount of time after which dialing "times out".

Item 1 is the one more likely to act as a separator here.

while (audio is coming in):
        run Goertzel
```

if DTMF detected and has been on longer than minimum time
record DTMF symbol
reset voice & silence timers
else if voice detected and has been detected longer than the minimum time:
record record separator
reset DTMF timer
else:
reset DTMF & voice timers
if silence has been on longer than minimum time:
record record separator

For each recorded symbol:
if there are no symbols in the potential number yet:
and the digit is between 2 an 9:
record symbol in potential number
and this is the first digit we've looked at and it's a 1:
skip to next symbol
otherwise, empty potential buffer and read to the next record separator
if there are less than 10 symbols in the potential number buffer:
and the symbol we're examining is in the range 0-9:
record symbol in potential buffer
otherwise, empty potential buffer and read to next record separator
if there are 10 symbol in the potential buffer:

and the symbol under examination is a record separator or (the symbol
under examination is '#' and the next symbol is a record
separator):
record the potential number as a detected number
otherwise, empty potential buffer and read to the next record separator

Note that although this is presented here and implemented in this program as
two distinct stages (parse audio, then parse symbols), there is nothing
preventing both parts from being run at the same time. That is, there is no
reason differentiation between valid envelope data and content data cannot
happen at the same time as the detection of DTMF symbols.

Goertzel Implementation based on text of
http://www.embedded.com/design/configurable-systems/4024443/The-Goertzel-Algorithm
and verified against the sample output there. There are slight rounding
mismatches, but nothing significant.

Using the following as the end of a gstreamer-1.0 pipeline will convert audio
into a format usable by this tool:
! audioconvert ! audioresample ! audio/x-raw, rate=8000, format=S8 ! \
filesink location=file.raw

```
Compile as:  cc -g -D_XOPEN_SOURCE=700 -
std=c99 -lm -o ccad ccad.c
*/

#include <stdlib.h>
#include <math.h>
#include <stdio.h>
#include <stdint.h>
#include <stdbool.h>
#include <errno.h>
#include <string.h>
#if      _POSIX_C_SOURCE      >=      2      ||
_XOPEN_SOURCE
#include <unistd.h>
#else
#error getopt not supported on this system
#endif
#if  _SVID_SOURCE  ||  _BSD_SOURCE  ||
_POSIX_C_SOURCE >= 200809L || \
            _XOPEN_SOURCE >= 700
#include <strings.h>
#else
#error ffs() not supported on this system
#endif

#define SAMPLE int8_t

#define LOG_DEFAULT 0
#define LOG_VERBOSE 1
#define LOG_DEBUG    2
#define log(level, ...) if (log_level>=level) \
        fprintf(log_output_file, __VA_ARGS__);

uint8_t log_level = 0;
FILE *log_output_file;
```

```
#ifndef M_PI
#define M_PI (3.14159265358979323846)
#endif

// All times measured in msec
#define SAMPLE_RATE                    8000   // Hz

#define N                              205    //105
is minimum for DTMF detection

        //205 frequently used/standard
#define SAMPLE_LENGTH
        ((float)N/SAMPLE_RATE)*1000//in msec

#define MAX_INTERDIGIT_TIME     10  *  1000
        // milliseconds
#define MIN_DIGIT_ON_TIME 40    //
milliseconds
#define MAX_DIGIT_INTERRUPT     10     //
milliseconds
#define MIN_VOICE_ON_TIME       1*1000     -
0*SAMPLE_LENGTH     //milliseconds

#define THRESH_DTMF 14
#define THRESH_VOICE -25 //-25 for wavs and
white noise, -37 for wavs & silence

// Coefficient (k) calculated from DTMF frequency
via k=N(fi/fs), where:
//  N is the constant filter length
//  fi is the DTMF frequency
//  fs is the sampling frequency
#define k(freq)                        (int)(0.5 + ((
(float)N * freq ) / SAMPLE_RATE))
```

```
#define coeff(freq)
        2*cos((2.0*M_PI*k(freq))/(float)N)

static float DTMF_TONES[8] = { 697, 770, 852, 941,
1209, 1336, 1477, 1633 };

/* The following encodes DTMF on/off state into a
byte using the index of the
 * tone in DTMF_TONES
 */
#define TONESTATE       uint8_t
#define TONESET(a, t)    (a |= (1<<t))
#define TONECLEAR(a, t)         (a &= ~(1<<t))
#define TONEISSET(a, t) (a>>t & 1)

static char DTMF2CHAR[5][5] = {
        /* row    { none, 1209 , 1336, 1477, 1633 }, */
        /* none */ {' ', ' ', ' ', ' '},
        /* 697 */ {' ', '1', '2', '3', 'A'},
        /* 770 */ {' ', '4', '5', '6', 'B'},
        /* 852 */ {' ', '7', '8', '9', 'C'},
        /* 941 */ {' ', '*', '0', '#', 'D'},
};

// The base size of the symbol buffer - where it starts
& how much it grows by
#define SYMBOL_BUFFER_UNIT_SIZE       100

// Used to keep track of symbols as they're detected
for later processing
char *symbol_buffer;
int                 symbol_buffer_length                =
SYMBOL_BUFFER_UNIT_SIZE;
int symbol_buffer_used = 0;
```

```
/*
Convert a TONESTATE to the human-readable character-equivalent.
*/
char state_to_char(TONESTATE state)
{
	TONESTATE upper = state >> 4 & 0xF;
	TONESTATE lower = state & 0xF;

	return DTMF2CHAR[ffs(lower)][ffs(upper)];
}

/*
Convert the magnitude output of Goertzel into dBFS.  dBFS is decibels relative
to the max output (volume/voltage/whatever) without clipping.  Since we're in
digital-land, this is easy - the max number that can be stored in the space
used for a single (audio) sample (ie: 8 bits).
*/
float rms2db(float mag)
{
	//RMS power = 0.707 * Peak Power
	//All our measurements are relative to max RMS power
	return 20 * log10(fabs(mag) /
			(powf(2, (sizeof(SAMPLE) * 8) - 1) * 0.707));
}

/*
Perform Goertzel algorithm on the specified set of N samples for the coefficient
passed in.
```

```
sqrt() is in there to scale the value back down to a
reasonable range.
*/
float goertzel(SAMPLE * samples, float coeff)
{
        float Q1 = 0, Q2 = 0;
        for (int i = 0; i < N; i++) {
                // Copy variables for cycle
                float Q0 = coeff * Q1 - Q2 +
(float)samples[i];
                Q2 = Q1;
                Q1 = Q0;
        }

        return sqrtf((Q1 * Q1 + Q2 * Q2 - Q1 * Q2 *
coeff) / (N / 2));
}

#define VAD_DECAY_RATE    0.37    //0.37    for
wavs and noise, wavs and silence
float rms_avg = 0;
/*
Compute RMS of a set of SAMPLEs, then updates
the running average.  Returns
true if there is sufficient activation to believe there
could be voice
content.
*/
bool has_voice(SAMPLE * sample)
{
        float res = 0;
        for (int i = 0; i < N; i++) {
                res += sample[i] * sample[i];
        }
        rms_avg =
```

```
            (VAD_DECAY_RATE) * sqrt(res / N) +
rms_avg * (1 - VAD_DECAY_RATE);
        log(LOG_DEBUG,      "RMS(sample):      %f,
RMS(avg):%f\n", sqrt(res / N),
            rms_avg);
        log(LOG_DEBUG, "RMS dB: sample: %f,
average: %f\n",
            rms2db(sqrt(res / N)), rms2db(rms_avg));
        return              (rms2db(rms_avg)            >
THRESH_VOICE);
}

/*
Wrapper around fread() to prevent partial reads
from causing failure, if not at
EOF.
*/
bool read_file(SAMPLE * buffer, FILE * infile)
{
        int count = N;
        while (count > 0 && !feof(infile)) {
                count               -=              fread(buffer,
sizeof(SAMPLE), count, infile);
        }
        if (count > 0) {
                if (feof(infile)) {
                        return false;
                }
        }
        return true;
}

/*
Runs various tests to determine if the tone
detection is genuine.  Detection
```

```
could also have been triggered by, for example, voice content.  This means
checking the first harmonic - this will be populated in voice, but not by
computer/mechanically generated tones.
*/
TONESTATE verify_tones(TONESTATE state, SAMPLE * buffer)
{
	for (int i = 0; i < 8; i++) {
		if (TONEISSET(state, i)) {
			if (rms2db(goertzel(buffer, coeff(DTMF_TONES[i] * 2))) >
				THRESH_DTMF) {
				log(LOG_DEBUG,
				  "Clearing tone %f; found 1st harmonic\n",
				  DTMF_TONES[i]);
				TONECLEAR(state, i);
			}
		}
	}
	return state;
}

/*
Verifies that the tone results are a valid result (ie: are a DTMF tone).
*/
bool verify_state(TONESTATE state)
{
	log(LOG_DEBUG, "%s: input: 0x%2x\n", __func__, state);
	TONESTATE upper = state >> 4 & 0xF;
	TONESTATE lower = state & 0xF;
```

```
        log(LOG_DEBUG, "%s: upper: 0x%2x\n",
__func__, upper);
        log(LOG_DEBUG, "%s: lower: 0x%2x\n",
__func__, lower);
        // Check 1: Bits set in both upper and lower
        if (upper == 0 || lower == 0) {
                log(LOG_DEBUG,
                   "Rejected state; not tones in both
upper & lower ranges\n");
                return false;
        }

        // Check 2: only one bit set in upper & lower
        TONECLEAR(upper, ffs(upper) - 1);
        TONECLEAR(lower, ffs(lower) - 1);
        log(LOG_DEBUG, "%s: upper: 0x%2x\n",
__func__, upper);
        log(LOG_DEBUG, "%s: lower: 0x%2x\n",
__func__, lower);

        if (upper != 0 || lower != 0) {
                log(LOG_DEBUG, "Rejected state; too
many bits set\n");
                return false;
        }

        return true;
}

float on_time = 0;
float off_time = 0;
float voice_time = 0;
char on_char = '\0';
bool emitted = false;
```

```
/*
Manages printing of result chars so they only get
printed once per instance.
*/
void emit(char x)
{
        if (!emitted) {
                if (log_level < LOG_VERBOSE ||
log_output_file != stdout) {
                        printf("%c", x);
                }
                // Now symbol buffer stuff
                symbol_buffer[symbol_buffer_used] =
x;
                symbol_buffer_used++;
                if (symbol_buffer_used >=
symbol_buffer_length) {
                        symbol_buffer =
realloc(symbol_buffer,

        symbol_buffer_length +

        SYMBOL_BUFFER_UNIT_SIZE);
                        memset(symbol_buffer +
symbol_buffer_used, 0,

SYMBOL_BUFFER_UNIT_SIZE);
                        symbol_buffer_length +=
SYMBOL_BUFFER_UNIT_SIZE;
                }
                emitted = true;
        }
}

/*
```

```
Resets printing result characters.  Prints timing
information.
*/
void reset(void)
{
        if (emitted) {
                log(LOG_VERBOSE, "%c: Active: %f,
silent: %f, voice: %f\n",
                        (on_char) ? on_char : '.',
on_time, off_time, voice_time);
        }
        on_char = '\0';
        on_time = 0;
        off_time = 0;
        voice_time = 0;
        emitted = false;
}

/*
Called if the sample does not have a DTMF tone in
it.  Resets, emits if long
enough apart we're sure the tone is done.
*/
void is_off(SAMPLE * buffer)
{
        if (has_voice(buffer)) {
                log(LOG_DEBUG,          "Voice
detected\n");
                voice_time += SAMPLE_LENGTH;
                log(LOG_DEBUG, "Voice on time:
%f\n", voice_time);
                if          (voice_time          >
MIN_VOICE_ON_TIME) {
                        emit('.');
                }
```

```
        }
        off_time += SAMPLE_LENGTH;
        if (on_char != '\0' && off_time >
MAX_DIGIT_INTERRUPT) {
                //Digit just timed out.
                emit(on_char);
                reset();
        }
        if (off_time > MAX_INTERDIGIT_TIME) {
                // Long off - separate inputs
                emit('.');
        }
}

/*
Called if the sample has a DTMF tone.  Manages
emitting if the tone has been on
long enough.  Manages emitting if changing tones.
NB: The standard (Q.23 & Q.24) specifies a min. 40
ms break between tones.  Not
everyone implements this, so we do not force such
a break.
*/
void is_on(char c)
{
        if (on_time == 0)
                reset();
        if (c != on_char && on_char != '\0') {
                emit(on_char);
                reset();
        }
        on_char = c;
        on_time += SAMPLE_LENGTH;
        if (on_time > MIN_DIGIT_ON_TIME)
                emit(on_char);
```

```
}

/* Stage 1 - filter audio into a symbol stream */
void stage1(FILE * infile)
{
        SAMPLE buffer[N];
        while (read_file(buffer, infile)) {
                TONESTATE state = 0;

                // For this set of samples, check each
frequency
                for (int i = 0; i < 8; i++) {
                        float res = goertzel(buffer,
coeff(DTMF_TONES[i]));
                        log(LOG_DEBUG, "%f, %.5f,
%.5f\n", DTMF_TONES[i], res,
                           rms2db(res));
                        if (rms2db(res) >
THRESH_DTMF) {
                                log(LOG_DEBUG,
"Frequency %.1f detected\n",
                                   DTMF_TONES[i]);
                                TONESET(state, i);
                        }
                }

                if (state) {
                        // First tone filtering:
                        state = verify_tones(state,
buffer);
                        // Second "logical filtering"
                        if (verify_state(state)) {
                                //Third, it's valid
                                log(LOG_DEBUG,
"Detected DTMF \"%c\"\n",
```

```
                                        state_to_char(state));

        is_on(state_to_char(state));
                        } else {
                                is_off(buffer);
                        }
                } else {
                        is_off(buffer);
                }
        }
}

/*
Given a pointer to a string, this function operates on the string to determine
if it contains a valid NANP number.  When it returns, returns a pointer
guaranteed to be pointing at either . or \0
*/
char *validate_num(char *buffer)
{
        char *start = buffer;
        char pot_num[15] = { 0 };
        int pos = 0;

        // While not at a separator
        while (*buffer != '.') {
                if (pos == 0 && start == buffer) {
        //if we haven't examined any digits...
                        if (*buffer == '1') {  // and we're looking at at 1
                                buffer++;     //move to the next entry
                                continue;     // and the next iteration
```

```
                } else if (*buffer >= '2' &&
*buffer <= '9') {       // and we're
                        // looking at something in
the range 2-9
                        pot_num[pos] = *buffer;
        // record the entry
                        pos++;
                } else {// empty buffer and not 1
or 2-9 means invalid number
                        break;// Move to next
possible number
                }
            } else if (pos == 0 && (*buffer == '1' ||
*buffer == '0')) {
                // NANP numbers may not start
with 0 or 1 and this is not positioned
                // so it could be the long-
distance 1.  Invalid number
                break;
            } else if (pos == 10 && *buffer == '#'
&& buffer[1] == '.') {
                // If we have 10 digits and are
looking at a separator or a #
                // followed by a separator:
                buffer++;       // move on to the .
                break;
            } else {
                if (pos < 10 && *buffer >= '0'
&& *buffer <= '9') {
                        // not the first pos and not
a full 10 digits and looking at 0-9
                        // -> add to buffer and
move on
                        pot_num[pos] = *buffer;
                        pos++;
```

```
                        } else {
                                break;// Fell through somehow.  Too many digits or one that
                                // isn't 0-9
                        }
                }
                // Move to the next character
                buffer++;
        }

        if (pos == 10 && *buffer == '.') {
                pot_num[pos] = '\0';        //end of string
                printf("%s\n", pot_num); // Print as a valid result
        }
        // If we got here, we're either ready to move on or need to read until
        // ready to move on
        while (*buffer != 0 && *buffer != '.') {
                buffer++;
        }
        return buffer;
}

/* Filter stage 2 - parse symbol stream for "acceptable" formats. */
void stage2(void)
{
        char *buffer = symbol_buffer;
        while (*buffer != '\0') {
                buffer = validate_num(buffer) + 1;
        }
}
```

```
/*
Main function (entry point) of the program. Manages parsing command line
options and very high level program flow.
*/
int main(int argc, char **argv)
{
	symbol_buffer = calloc(symbol_buffer_length, sizeof(char));
	log_output_file = stdout;
	char c;
	while ((c = getopt(argc, argv, "hdv2")) != -1) {
		switch (c) {
		case 'h':
			exit(0);
			break;
		case 'd':
			log_level = LOG_DEBUG;
			break;
		case 'v':
			log_level = LOG_VERBOSE;
			break;
		case '2':
			log_output_file = stderr;
			break;
		}
	}

	log(LOG_VERBOSE, "Starting with sample rate of %d hz, block size %d\n",
	    SAMPLE_RATE, N);
	log(LOG_VERBOSE, "Sample length is %fmsec\n", SAMPLE_LENGTH);

	FILE *infile;
```

```
	if (optind < argc) {
		log(LOG_VERBOSE, "Reading input
file %s\n", argv[optind]);
		errno = 0;
		infile = fopen(argv[optind], "r");
		if (errno) {
			perror(NULL);
			exit(1);
		}
	} else {
		log(LOG_VERBOSE, "Using stdin
%d\n", argc);
		infile = stdin;
	}

	// Stage 1 processing
	stage1(infile);

	// Make the symbol buffer end in a .
	reset();
	emit('.');
	printf("\n");		//Separate stage1 output
from stage2

	//Stage 2 processing
	stage2();

	//cleanup
	free(symbol_buffer);
	if (infile != stdin)
		fclose(infile);
}
```