2000

Is Big Brother Listening--A Critical Analysis of New Rules Permitting Law Enforcement Agencies to Use Dialed Digit Extraction

Michael A. Rosow

Follow this and additional works at: https://scholarship.law.umn.edu/mlr

Part of the Law Commons

Recommended Citation

This Article is brought to you for free and open access by the University of Minnesota Law School. It has been accepted for inclusion in Minnesota Law Review collection by an authorized administrator of the Scholarship Repository. For more information, please contact lenzx009@umn.edu.
Imagine working for a large company under investigation for serious criminal activity. The Federal Bureau of Investigation (FBI) has convinced a judge to issue a warrant allowing agents to see the phone numbers of every individual who receives a phone call from your office or any mobile phone billed to your office, but has refused to issue a warrant allowing the FBI to listen to those conversations. While driving home from work, you make a call from your company mobile phone to the local pharmacy and reach an automated system. When the computer-generated voice asks for your prescription number, you dial in your prescription for AZT, the HIV cocktail medication. You stop at the pharmacy and pick up your prescription half an hour later. The following week you are approached by a FBI agent who demands that you provide inside information for the investigation. When you refuse to provide this information, the agent threatens to tell your parents, your boss, and your pastor that you have HIV. Although this scenario may seem far-fetched, new rules issued by the Federal Communications Commission (FCC) on August 31, 1999 would enable the FBI to do this very thing.

The device used by law enforcement agencies to obtain the numbers dialed from a telephone is a pen register. Currently a pen register can only intercept the first set of numbers dialed from a telephone. Under the new rules, which become effective on September 30, 2001, law enforcement agencies will have ac-
cess to digits dialed after the telephone call has been connected (dialed digit extraction). This new development raises serious issues regarding the constitutionality of these rules and the FCC's authority to enact them. Privacy groups and the telecommunications industry argue that the rules substantially increase the type and amount of information available via a pen register. Law enforcement agencies, on the other hand, argue that this capability merely allows them to keep pace with changing technology.

This Note will examine the statutory validity and constitutionality of the new rules authorizing the use of dialed digit extraction by law enforcement. Part I describes the technology at issue, the statutory framework under which the rules were issued, and the constitutional framework under which the rules should be analyzed. In Part II, this Note argues that the FCC exceeded its authority in issuing these rules and that the rules are unconstitutional under the Fourth Amendment. This Note concludes by suggesting alternatives that may resolve the issues more suitably while still providing necessary information to law enforcement agencies.

I. TECHNICAL, STATUTORY AND CONSTITUTIONAL SIGNIFICANCE OF A PEN REGISTER

A. TECHNICAL DIFFERENCE BETWEEN A WIRETAP AND A PEN REGISTER

Although three types of electronic surveillance devices are available: wiretaps, pen registers, and trap and trace devices, this Part will only examine the differences between wiretaps and pen registers. The difference between these two devices is initially important for practical reasons; there is a radical difference between the type and amount of information obtained


4. This Note avoids extensive discussion of trap and trace devices, but due to their similarity with pen registers, they will be discussed tangentially. A trap and trace device works like a caller ID box installed by a third party. The device "captures the incoming electronic or other impulses which identify the originating number" from which a telephone call was made. 18 U.S.C. § 3127(4) (1994).
from a wiretap as opposed to a pen register. Due to this difference, wiretaps and pen registers are subject to different standards.

Government-conducted wiretaps are governed primarily by Title III of the Omnibus Crime Control and Safe Streets Act of 1968. A Title III wiretap allows law enforcement agencies to listen to the "content" of telephone conversations. The criteria used to determine what exactly constitutes "content" is central to the distinction between Title III wiretaps and pen registers and will be discussed in detail later in this Note. For now, it is sufficient to note that conversations between two different parties constitute call "content," while the numbers dialed to connect a call do not. In contrast to a wiretap, a pen register does not obtain call "content," but only records the phone number of the called party. A wiretap also obtains the numbers dialed on a telephone, but accomplishes this task in a different manner.

7. See United States v. Kail, 612 F.2d 443, 446 (9th Cir. 1979).
9. Compare Smith v. Maryland, 442 U.S. 735, 745-46 (1979) (holding that since a pen register did not obtain the "content" of a telephone call it was not a "search and seizure" under the Fourth Amendment), and New York Tel. Co., 434 U.S. at 167 (holding that a pen register did not intercept because it did not obtain call "content"), with Katz, 389 U.S. at 359 (holding that listening to the telephone call of an individual constitutes a "search and seizure" under the Fourth Amendment), and Kail, 612 F.2d at 447 (holding that once a valid wiretap order has been issued law enforcement agencies do not need to obtain additional authorization to use a pen register).
10. See infra note 133 and accompanying text.
12. See Smith, 442 U.S. at 736 n.1 (citing New York Tel. Co., 434 U.S. at 161 n.1); see also Michigan Bell Tel. Co. v. United States, 565 F.2d 385, 386 (6th Cir. 1977) ("[A] pen register only records the telephone numbers dialed by a monitored telephone."). A pen register performs a very limited function. It does not record or monitor the contents of a call and does not indicate whether or not the call was completed. See id. at 386 n.1 (citing United States v. Giordano, 416 U.S. 505, 549 (1974) (Powell, J., concurring in part and dissenting in part)).
13. See Kail, 612 F.2d at 448. Since a Title III wiretap records the electrical impulses that identify numbers dialed on a telephone, it is possible to decipher these numbers without the use of a pen register. See id. The "mechanical refinement provided by the pen register is thus comprehended within the terms of the wiretap order, making separate authorization unnecessary." Id.
Pen registers gather different types and amounts of information as compared to wiretaps because the current telephone switching system prevents pen registers from intercepting the content of telephone communications. Modern telephone switching systems have at least two different channels for a simple telephone communication. The first channel, the call data channel, routes the call through to the proper location and remains operational only until the phone call has been properly routed, which occurs when it rings on the other end of the line. The call is routed at a switch into which tone receivers are built and when the call is routed over this first channel, the call goes through the tone receivers. The switch employs tone receivers to detect the dialed digits representing the phone number. It then connects the call, at which point the call is "cut through." After the communication has been cut through the tone receiver disconnects from the switch and is available for use on another call. At this point, the conversation is transferred along the "call content channel." There are fewer tone receivers built into a switch than there are call content channels. Therefore, a single switch may service more simultaneous communications than it has tone receivers because the majority of the communications going through a switch, at any given time, have been cut through and are being carried along the call content channel instead of the call data channel.

(citation omitted).

14. See 18 U.S.C. § 3127(3) (defining a pen register as "a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached").

15. See Michael W. Mowery, Comments of Airtouch Communications, Inc. at 18 (No. 97-213) (May 20, 1998) [hereinafter May Airtouch Petition].


17. See id.

18. See id.

19. See id.


21. See May TIA Petition, supra note 16, at 44 ("Because tone receivers can be repeatedly used in this manner, manufacturers build switches with a number of tone receivers that is far lower than the number of simultaneous calls that the switch can support.").
B. AN HISTORICAL SURVEY OF THE LAW ON WIRETAPPING AND USE OF PEN REGISTERS

In the last half-century there have been three major statutory changes to the laws of wiretapping and pen registers. While this Note focuses on the rules enacted subsequent to the Communications Assistance for Law Enforcement Act of 1994 (CALEA), it is important to understand the progression of the law through the latter half of the twentieth century because CALEA builds upon these other acts.

1. The Omnibus Crime Control and Safe Street Act of 1968

The first statute, Title III of the Omnibus Crime Control and Safe Street Act of 1968, made it illegal for an individual to conduct electronic surveillance, but made it possible for law enforcement agencies to obtain judicial authorization to engage in such surveillance. Title III was primarily a response to advancements in technology. Title III had a dual purpose of protecting telephone communications from unauthorized interception and delineating the proper circumstances and conditions for conducting telephone surveillance.

The standards that Title III set for obtaining a wiretap have remained virtually unchanged in the three decades since its enactment. In order to issue a warrant, a judge must find that "there is probable cause [to believe] that an individual is committing, has committed, or is about to commit a particular offense . . . [and that] normal investigative procedures have been tried and have failed or reasonably appear to be unlikely


25. See H.R. REP. No. 103-827, at 11 (1994) ("[T]he tremendous scientific and technological developments that have taken place in the last century have made possible today the widespread use and abuse of electronic surveillance techniques. As a result of these developments, privacy of communications is seriously jeopardized by these techniques of surveillance.") (quoting S. REP. No. 90-1097, at 67 (1968)).

26. See id.
to succeed if tried or to be too dangerous."^{27} However, Title III did not initially address pen registers or set a standard to issue a warrant for a pen register.\textsuperscript{28}

Title III was amended slightly in 1970 after the Ninth Circuit held that telephone companies were not required to assist law enforcement agencies in effectuating electronic surveillance.\textsuperscript{29} This ruling paralyzed law enforcement agencies; they could obtain a valid warrant for a Title III wiretap, but were helpless to effectuate it without the assistance of the telecommunications companies.\textsuperscript{30} Without this assistance, law enforcement would have to set up their wiretaps in plain view of the subject of the tap. But in order to be effective, law enforcement needed to be able to conduct these taps secretly.\textsuperscript{31}

The amendments required telephone companies to furnish the law enforcement agency requesting assistance with "all information, facilities, and technical assistance necessary to accomplish the interception."\textsuperscript{32} This allowed law enforcement agencies to lease lines from the telecommunications companies so that they could conduct their taps without being observed.\textsuperscript{33}

2. The Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act of 1986 (ECPA) made several relevant changes to Title III. First, it ex-
tended the protections of Title III to "include electronic mail, cellular phones, computer transmissions of data or video, and voice or display paging devices." However, Congress somewhat negated the impact of this amendment by not extending access to these new technologies, which in effect allowed technology to outpace law enforcement's ability to conduct electronic surveillance. So while these new forms of communication were protected from being tapped without a warrant, the statute did nothing to ensure that telecommunications companies would continue to design their systems in a manner that facilitated electronic surveillance by law enforcement agencies.

ECPA also added new provisions to the code concerning the use of pen register devices. It amended Title III to create the first mandatory federal procedures for obtaining a pen register warrant. Previously, pen registers were issued under the court's general power to issue warrants. Now, an order for a pen register may be issued only after a showing that "the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." Conversely, a Title III wiretap can only be obtained after meeting the much more stringent "probable cause" standard.

37. See id.
39. 18 U.S.C. § 3122(b)(2). Note that these requirements are very different from the requirements necessary to obtain a wiretap: (a) the identity of the law enforcement officer making the application; (b) a statement of the facts and circumstances relied upon by the applicant, including a detailed description of the particular offenses alleged, the location of the intercept, and the types of communications to be intercepted, and the identity of the persons whose communications are to be intercepted; (c) an explanation of why other investigative measures have failed or why they are unlikely to be successful; (d) a statement of the time for which the interception will be active; (e) a statement of all previous applications for electronic surveillance of the same individual; and (f) where the application is for an extension, a statement setting forth the information so far obtained. See id.
40. See id. § 2518(3); see also supra note 27 and accompanying text.
3. The Communications Assistance for Law Enforcement Act of 1994 (CALEA)

a. The Path to CALEA

As the 1980s progressed, the law enforcement community began to realize that it was losing its ability to conduct electronic surveillance. Technological developments were making it increasingly difficult for Title III wiretaps and pen registers to be used effectively. Prior to the breakup of AT&T, the telecommunications system was quite simple. The network consisted mainly of stationary telephones that were connected by land-based wires to stationary switching stations. To install a Title III wiretap or a pen register, a law enforcement agency only had to find a location where the wires were exposed and either: (1) attach a listening/recording device to that location; or (2) rent another phone line and send the tapped conversation to a distant location to be listened to and recorded.

After the breakup of AT&T, however, a massive technological revolution occurred in the telecommunications industry. Now fiber-optic cables are replacing the old copper cables, and computers are replacing traditional switches. Mobile phones are not connected to any fixed location and can roam around the country sending their signal through different switches wherever they go. In addition, companies are adding new features to traditional telephones that allow a single telephone number to ring in several different places or that allow a user to dial an abbreviated directory number to call another party.

41. See U.S. CONG. OFFICE OF TECH. ASSESSMENT, ELECTRONIC SURVEILLANCE IN A DIGITAL AGE 2 (1995) [hereinafter ELECTRONIC SURVEILLANCE].
42. See id.
43. See id.
44. See id. at 1 (“When the telephone system was largely a network that connected handsets like the plain old black rotary dial telephones, wiretapping was largely a simple procedure of physically connecting a listening or monitoring device to a circuit associated with a telephone number. It was simple and inexpensive.”).
45. See id. at 1-2.
46. See id. at 2.
47. See id. at 42-50 (describing the problems with finding a fixed location for cellular phones and for Personal Communication Services (PCS) phones).
48. See id. at 40.
49. See id. at 39.
In total, these advanced features have made it more difficult for law enforcement agencies to conduct electronic surveillance.\(^5\)

In response to these technological developments, the Clinton administration introduced a proposal that would eventually lead to CALEA.\(^5\) At the congressional hearings, the proposal was met with both support and opposition.\(^5\) Opposition to the bill came from privacy advocate groups and the telecommunications industry.\(^3\) The privacy advocate groups focused on the threat the bill posed to the privacy of communications.\(^3\) The telephone industry emphasized the lack of need for the new legislation and the cost of the new mandates on telephone carriers.\(^5\) The industry claimed that the FBI was overstating any problems that it had in effectuating wiretaps.\(^6\)

In support of the proposal, FBI Director Freeh spoke on behalf of the law enforcement community. He hypothesized that a parade of horribles would result if Congress did not act to strengthen law enforcement's ability to conduct electronic surveillance.\(^5\) Freeh also indicated that the proposed bill

\(^5\). See Hearings, supra note 35, at 5-35 (statement of Louis J. Freeh, Director, Federal Bureau of Investigation). But see id. at 57, 65-78 (statement of Roy Neel, President, U.S. Telephone Association) (stating that he “is aware of only a handful of instances in which there has been difficulty in providing assistance [to law enforcement agencies]”); id. at 70 (statement of Jerry Bergman, Executive Director, Electronic Frontier Foundation) (stating that “there is no evidence that current law enforcement efforts are being jeopardized by new technologies... [and the] industry is cooperating with appropriate authorities to avoid future problems and to expand existing capacities”).

\(^5\) See BeVier, supra note 34, at 1069, 1075-77.

\(^5\) See H.R. REP. NO. 103-827, at 10-11 (1994). See generally S. REP. NO. 103-402 (1994). Since the hearings were conducted jointly the reports are almost identical. This Note will only cite to the House Report unless there is a major difference between the two reports.

\(^5\) See BeVier, supra note 34, at 1077.

\(^5\) See Hearings, supra note 35, at 65-78 (statement of Jerry Bergman, Executive Director, Electronic Frontier Foundation). Bergman also raised cost and certainty issues. See id. at 69-70. He argued that the bill imposed uncertain requirements on mobile telephone providers and that the cost reimbursement provisions were not adequate. See id. at 69.

\(^5\) See id. at 53-64 (statement of Roy Neel, President, U.S. Telephone Association).

\(^5\) See id. at 57. Speaking for the telephone industry, Roy Neel stated that he “was not aware of a single instance in which a wire line local telephone company has not been able to effect a lawful intercept due to complications related to advancements in technology.” Id.

\(^5\) See id. at 17-21 (statement of Louis J. Freeh, Director, Federal Bureau of Investigation). Specifically, Freeh provided a long list of what was to come
would not increase the type or amount of information that law enforcement was able to obtain.58

During the congressional debates leading up to the passage of CALEA, Congress seemed to agree with Director Freeh, and stated that the purpose of CALEA is "to further define the industry duty to cooperate [with law enforcement agencies] and to establish procedures based on public accountability and industry standards-setting."59 Congress made it clear that it was carefully balancing three key policies: "(1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies."60

b. Provisions of CALEA

The provisions of CALEA attempt to balance the triad of sometimes-conflicting policies that Congress identified in passing CALEA. CALEA not only imposes new requirements on telephone carriers, but also imposes new restrictions on the type of information that can be obtained by law enforcement agencies using particular methods of electronic surveillance.61 Pursuant to its purpose, CALEA attempts to simultaneously balance law enforcement's ability to conduct surveillance with privacy concerns, while still allowing telephone carriers to develop new communication services and technologies.62 These

58. See id. at 16. Freeh stressed that the legislation would only provide law enforcement agencies with information that they had typically received from electronic surveillance. See id. In many ways Freeh seemed to imply that the legislation was just a technology update to outdated laws. See id.


60. Id. at 13.


various interests are often intertwined and difficult to separate. This section will describe the changes that CALEA made to Title III and ECPA by proceeding from the general changes to the specific.

CALEA requires that wireline, cellular, and Personal Communication Services (PCS) comply with four general capability requirements.\(^{63}\) Telecommunications carriers are to be capable of: (1) quickly obtaining, for government use, specific communications pursuant to a court order;\(^{64}\) (2) quickly allowing the government access to "call-identifying information that is reasonably available;"\(^{65}\) (3) delivering the intercepted communications and call-identifying information to the government over equipment provided by the carrier for the government;\(^{66}\) and (4) providing the previous functions without interference to telecommunication services and preventing unauthorized interceptions.\(^{67}\)

Two terms in the second clause of the capability requirements are crucial to understanding the limits placed on law enforcement's ability to conduct electronic surveillance: (1) the definition of call-identifying information; and (2) what makes the information reasonably available. Call-identifying information is defined as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier."\(^{68}\) Based on the legislative history, it is clear that Congress intended this term to be narrowly tailored. Call-identifying information was limited to those "pulses, tones, or messages [that] identify the numbers dialed from the facility that is the subject of the court order or other lawful authorization."\(^{69}\) Numbers dialed for other purposes, such as communicating with the called party, are not considered call-identifying information.\(^{70}\)

Unfortunately, the statute does not define the term "reasonably available" in the context of call-identifying information.

---

\(^{64}\) See id. § 1002(a)(1).
\(^{65}\) Id. § 1002(a)(2).
\(^{66}\) See id. § 1003(a)(3).
\(^{67}\) See id. § 1003(a)(4).
\(^{68}\) Id. § 1001(2).
\(^{69}\) H.R. REP. NO. 103-827, at 21.
\(^{70}\) See id.
The term reasonably available limits the amount of call-identifying information available to law enforcement agencies. However, without a definition, the FCC and the courts are left to interpret this vague term without any direct guidance. It is unclear what factors the legislature was taking into account when it attempted to limit the availability of call-identifying information. The statute does, however, provide a list of factors including costs to be considered when determining if a capability is "reasonably achievable." While not identical, this term is similar and may be useful in providing some context for what Congress was thinking when it used the term reasonably available.

CALEA also imposes a new limitation on the use of pen registers by law enforcement agencies. The statute calls for law enforcement agencies to use technology that was reasonably available to prevent pen registers from recording numbers other than those used in the dialing or signaling process. Prior to this amendment, the only factors that limited the use of pen registers were the process used to obtain a warrant and the definition of a pen register.

71. See 47 U.S.C. § 1008(b)(1). The factors to be considered are as follows:
   (A) The effect on public safety and national security.
   (B) The effect on rates for basic residential telephone service.
   (C) The need to protect the privacy and security of communications not authorized to be intercepted.
   (D) The need to achieve the capability assistance requirements of section 1002 of this title by cost-effective methods.
   (E) The effect on the nature and cost of the equipment, facility, or service at issue.
   (F) The effect on the operation of the equipment, facility, or service at issue.
   (G) The policy of the United States to encourage the provision of new technologies and services to the public.
   (H) The financial resources of the telecommunications carrier.
   (I) The effect on competition in the provision of telecommunications services.
   (J) The extent to which the design and development of the equipment, facility, or service was initiated before January 1, 1995.
   (K) Such other factors as the Commission determines are appropriate.

73. See id.
74. See id. §§ 3121(a), 3122, 3123.
75. See id. § 3127(3) ("[T]he term 'pen register' means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is at-
Finally, CALEA provides a safe harbor for telecommunications carriers that are "in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, or by the Commission." Once the industry has set standards, the Government or any other interested entity can petition the FCC to reject the industry standards and establish new technical requirements if the FCC finds that the industry standards are deficient. In setting technical requirements or standards the FCC must:

1. meet the assistance capability requirements of [47 U.S.C. § 1002] by cost-effective methods;
2. protect the privacy and security of communications not authorized to be intercepted;
3. minimize the cost of such compliance on residential ratepayers;
4. serve the policy of the United States to encourage the provision of new technologies and services to the public; and
5. provide a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of telecommunications carriers under [47 U.S.C. § 1002] during any transition period.

So while the telecommunications industry has the first chance to establish technical standards, the FCC is ultimately responsible for determining the final standards for the safe harbor.

c. The Standard-Setting Process

In 1995, members of the Telecommunications Industry Association (TIA) began establishing industry standards that would satisfy CALEA. Both telecommunications industry members and law enforcement agencies participated in this process. In the spring of 1997, proposed standards were submitted for balloting to all participants in the standard-setting process. The law enforcement community unanimously opposed the standards and prevented their adoption. Furthermore, the Department of Justice and the FBI submitted a draft...
of their own technical standards to satisfy CALEA. These standards became known as the “punch list” and contained nine items when reviewed by the FCC in the fall of 1998. The punch list contained a wide variety of items, but for the purposes of this Note only the last item is relevant.

The last item on the punch list required telecommunications carriers to provide dialed digit extraction. This new capability would allow law enforcement agencies to record any digits dialed after the call has been cut through. These numbers are known as post-cut-through numbers. In other words, law enforcement agencies would be able to obtain additional numbers provided to a long distance service provider, an automated system, a bank, voicemail, a paging device, or any other numbers dialed after connection.

The industry refused to add any of the punch list items to their standards and reballedot using a different voting method that excluded law enforcement representatives. The new standard, J-STD-025, was announced in December of 1997. Between July 1997 and April 1998, several parties petitioned for the FCC to establish standards for CALEA. The petitions ranged from requests to reject J-STD-025 to requests for the FCC to adopt J-STD-025, with some parties asking for it to be adopted with some alterations.

On April 20, 1998, the FCC released a Public Notice soliciting comment on the petitions. Numerous comments were filed pursuant to this request.

---

83. See id. ¶ 13.
84. See id.
85. When submitted to Commission, the Punch List contained nine items: (1) Content of subject-initiated conference calls; (2) Party hold, join, drop; (3) Subject-initiated dialing and signaling information; (4) In-band and out-of-band signaling (notification messages); (5) Timing information; (6) Surveillance status; (7) Continuity check tone (c-tone); (8) Feature status; and (9) Dialed digit extraction. See id. (citations omitted).
86. See id. ¶ 14.
87. See id. ¶ 15.
88. See id. ¶ 16.
89. The Cellular Telecommunications Industry Association, the Electronic Frontier Foundation, the Center for Democracy and Technology, the Department of Justice, the FBI, and the TIA all petitioned for the Commission to establish standards for CALEA. See id. ¶¶ 16-22.
90. See id. ¶¶ 16-19.
91. See id. ¶ 21.
92. See id.
93. See id.
On November 5, 1998, the FCC released the Further Notice of Proposed Rulemaking (Further NPRM). The Further NPRM tentatively concluded that J-STD-025 would be acceptable if TIA modified it to include five items from the punch list. The FCC requested further comment on whether the dialed digit extraction capability was necessary and tentatively rejected the other three items on the punch list.

After receiving another round of comments on the Further NPRM, the FCC promulgated the final rules on August 26, 1999. In addition to the requirements of J-STD-025, these rules ordered telecommunications carriers to provide law enforcement agencies with the five tentatively accepted punch list items and dialed digit extraction. The FCC considered and rejected arguments that dialed digit extraction is not permitted under CALEA. Alternative methods of obtaining "call-identification" information were also considered and rejected by the FCC. The FCC concluded that while it was "concerned about the costs of a dialed digit extraction capability to originating carriers, as well as the privacy implications of permitting [law enforcement agencies] to access non-call-identifying digits (such as bank account numbers) with only a pen register," it determined that permitting law enforcement agencies access to post-cut-through numbers was both constitutional and statutorily permitted.
C. FOURTH AMENDMENT PROTECTIONS AGAINST UNREASONABLE SEARCH AND SEIZURE AS APPLIED TO WIRETAPS AND CONVENTIONAL PEN REGISTERS

As noted previously, there is a substantial difference in the information obtained via a Title III wiretap as opposed to a pen register.\textsuperscript{104} Due to this radical difference, the Supreme Court has applied the Fourth Amendment to the two processes quite differently.

1. The Constitutionality of Wiretaps

The United States Supreme Court first addressed the constitutionality of wiretapping in Olmstead v. United States.\textsuperscript{105} The Court held that a wiretap, conducted without obtaining a warrant, did not violate the Fourth Amendment.\textsuperscript{106} The wiretap did not fall within the realm of a "search and seizure" as defined by the Fourth Amendment because the law enforcement agents never actually entered into a structure or searched any tangible items.\textsuperscript{107}

In 1967, the Supreme Court readdressed the issue of whether a federally conducted wiretap was constitutionally permissible.\textsuperscript{108} Previously, the Court had looked to determine if the search was in a private or public area.\textsuperscript{109} In Katz v. United States, however, the Court framed the issue in terms of

\textsuperscript{104} See supra notes 4-21 and accompanying text.

\textsuperscript{105} 277 U.S. 438 (1928) overruled in part by Berger v. United States, 388 U.S. 41 (1967), and Katz v. United States, 389 U.S. 347 (1967). At the time of the decision, there were no federal statutes on the issue of wiretapping. See id. at 465-66. The wiretap, however, was carried out in the state of Washington, where it was a misdemeanor for any person to "intercept, read or in any manner interrupt or delay the sending of a message over any telegraph or telephone line." Id. at 468 (quoting Remington Compiled Statutes § 2656-18) (1922)).

\textsuperscript{106} See id. at 464 ("The [Fourth] Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants."). But see id. at 478 (Brandeis, J., dissenting) ("To protect, that right [the right to be let alone,] every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.").

\textsuperscript{107} See id. at 464.

\textsuperscript{108} See Katz, 389 U.S. at 347. Katz had been convicted for violating 18 U.S.C. § 1804, which prohibited the interstate use of wire communications for use in the business of betting or wagering. See id. at 348-49. At trial the FBI introduced evidence which it collected by using a wiretap attached to a phone booth that Katz frequently used. See id.

\textsuperscript{109} See id. at 351.
whether the target had exposed information to the public.\textsuperscript{110} \textit{Katz} involved a wiretap placed on a public telephone.\textsuperscript{111} The Court found that the target of the search never exposed any information to the public and instead was attempting to keep his conversation private.\textsuperscript{112} In a reversal of \textit{Olmstead}, the Court held that the Fourth Amendment "protects people, not places."\textsuperscript{113} As a result, it was an invasion of privacy and an unconstitutional "search and seizure" within the meaning of the Fourth Amendment for law enforcement officials to wiretap a telephone booth without a warrant.\textsuperscript{114}

2. The Constitutionality of Pen Registers

Unlike wiretaps, pen registers are not subject to the Fourth Amendment protections against unreasonable searches and seizures.\textsuperscript{115} In finding that pen registers are not subject to Fourth Amendment protection, the Supreme Court applied a two-part test: (1) whether the individual "exhibited an actual subjective expectation of privacy," and (2) whether "society is prepared to recognize" that expectation of privacy as reasonable.\textsuperscript{116} The first prong is a subjective test, whereas the second is objective.\textsuperscript{117} With respect to the first prong, the Court held

\begin{itemize}
\item \textsuperscript{110} See id.
\item \textsuperscript{111} See id. at 348-49.
\item \textsuperscript{112} See id at 352. The Court specifically rejected the argument that because Katz was visible after he entered the phone booth he had forfeited his expectation of privacy. See id. Instead, the Court held that because Katz had "shut[ ] the door behind him, and [p]aid the toll that permits him to place a call" he was "entitled to assume that the words he utter[ed] into the mouthpiece [would] not be broadcast to the world." Id. In doing so, the Court implied that the Fourth Amendment's protection is an evolving concept. See id.
\item \textsuperscript{113} Id. at 351. The Court concluded "that the underpinnings of \textit{Olmstead} and \textit{Goldman} have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling." Id. at 353. Thus, the Court held that the act of listening to and recording the telephone conversation was key to determining the constitutionality of the activity instead of whether the police had penetrated the telephone booth during the wiretap. See id. at 351-53.
\item \textsuperscript{114} See id. at 353, 359.
\item \textsuperscript{116} Id. (quoting \textit{Katz}, 389 U.S. at 361 (Harlan, J., concurring)).
\item \textsuperscript{117} See id.
\end{itemize}
that individuals do not generally have "any actual expectation of privacy in the numbers they dial."\(^{118}\) Moreover, even if an individual had a "subjective expectation that the phone numbers he dialed would remain private, this expectation is not 'one that society is prepared to recognize as 'reasonable.'"\(^ {119}\) The Supreme Court concluded that there is "no legitimate expectation of privacy" in dialing information since it is turned over to a third party, namely the phone company.\(^ {120}\)

Because pen registers are not subject to Fourth Amendment protection, the constitutional requirements for obtaining a Title III wiretap are substantially higher than those for a pen register. In fact, the requirements for obtaining a pen register are encompassed by those for obtaining a Title III wiretap. This is partially due to the fact that the information received from a pen register can be gathered via a Title III wiretap. Given these facts, a court has held that no separate authorization is required for a pen register when authorization for a Title III wiretap has been obtained.\(^ {121}\)

II. DIALED DIGIT EXTRACTION: AN UNPERMITTED AND UNCONSTITUTIONAL PROCEDURE

The addition of dialed digit extraction to the J-STD-025 standard raises a number issues. First, it is not clear from the text of CALEA whether Congress contemplated dialed digit extraction when it passed the statute. Nor is it immediately clear whether CALEA authorizes or prohibits the use of dialed digit extraction; there are several statutory provisions that must be analyzed to resolve this issue. Resolving these questions must begin with the text of CALEA and then proceed to the legislative history and other related documents. Second, it is ques-

\(^{118}\) Id. at 742.

\(^{119}\) Id. at 743 (quoting \textit{Katz}, 389 U.S. at 361 (Harlan, J., concurring)).

\(^{120}\) Id. at 743-44. The Court based its conclusion on the assumption that telephone users are aware that they are communicating the telephone numbers that they dial to the telephone company and that the company has the capability to record this information and in fact does so for long distance phone calls. \textit{See} id. at 743. This may be even more true in the case of mobile phones. Most cellular or PCS phone bills indicate the numbers that were dialed from the phone and some even indicate the phone numbers of incoming calls.

\(^{121}\) \textit{See} United States v. Kail, 612 F.2d 443, 448 (9th Cir. 1979). In Kail, government agents installed a pen register without obtaining a separate warrant. \textit{See} id. The government agents had already obtained a warrant to conduct a wiretap. \textit{See} id.
tionable whether dialed digit extraction is constitutional. Because it is performed pursuant to a pen register warrant, it is disputed whether the information obtained via dialed digit extraction is protected by the Fourth Amendment or whether it is unprotected like telephone numbers.

This Part of the Note will argue that dialed digit extraction is not authorized by CALEA and is invalid under the Fourth Amendment. The current statutory framework prohibits law enforcement from obtaining post-cut-through numbers with only a pen register warrant. This Note will provide three distinct reasons why the text of CALEA prohibits dialed digit extraction. Additionally, this Note will argue that the rules permitting dialed digit extraction do not conform to the requirements of the Fourth Amendment. Thus, dialed digit extraction is not a valid exercise of FCC authority and must be rejected.

A. DIALED DIGIT EXTRACTION IS NOT AUTHORIZED BY CALEA

Whether CALEA authorized the use of dialed digit extraction using only a pen register depends on a three-part analysis. First, are post-cut-through numbers "call-identification information" as defined by CALEA? Second, are post-cut-through numbers reasonably available? Third, will the inclusion of dialed digit extraction meet the requirements of 47 U.S.C. § 1006(b)?122 If any of the questions are answered in the negative then dialed digit extraction must be rejected as unauthorized by CALEA.

1. Post-Cut-Through Numbers Are Not "Call-Identification Information"

Digits dialed after connection are not call-identifying information for several reasons. First, the numbers are not carried on the call data channel after the initial local carrier has connected the call123—the additional digits are carried over the

122. 47 U.S.C. § 1006(b) (1994) establishes criteria that the FCC must use when establishing a technical standard after it has been petitioned to do so. See supra notes 76-78 and accompanying text for a more detailed description of the requirements.

123. See supra notes 15-21 and accompanying text. This occurs when the initial number (1-800-XXX-XXXX) is dialed and the individual is connected to either the next carrier (a long distance provider), to an automated system, or to another individual.
A pen register is not authorized to obtain the content of a phone conversation. Thus, by definition, digits dialed after connection should not legally be subject to a pen register, because a pen register warrant is not authorized to intercept information that is carried on the call content channel.

Second, call-identification information is limited to “dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier.” Digits dialed after connection may serve one of two general functions. First, they may constitute another phone number that is dialed through another carriers' system. An example of this is a phone number placed through a long distance carrier after dialing an 800 number. Second, they may be numbers dialed to access an automated system. Examples of this include numbers dialed to access voice mail, bank records, a paging device and the internet. For the initial local carrier the first set of numbers identifies the direction, destination, and termination of the call. Once the call has been cut through to the secondary services provider the primary carrier does not re-direct the call, change its destination, or alter the call's termination point. The primary carrier directs the call to the secondary service provider for the entire call. If the primary carrier provides post-cut-through numbers, the primary carrier would be providing more than just call-identification information, because for the primary carrier's purposes, call-identification information is limited to the first set of numbers dialed.

Legislative history also indicates that Congress had no intention of providing post-cut-through numbers to law enforcement agencies via a pen register. Call-identifying information was limited to the numbers dialed to signal the telephone company where to direct the call. Other numbers dialed to

124. See supra notes 15-21 and accompanying text.
125. See supra notes 15-21 and accompanying text.
127. See supra notes 15-21 and accompanying text.
128. Secondary service providers include secondary carriers, such as AT&T or Sprint, and automated systems.
129. See supra notes 15-21 and accompanying text.
131. See id.
signal automated systems are not call-identification information. Post-cut-through numbers are "other dialing tones" as described by Congress and should be excluded from the definition of call-identifying information. Moreover, it does not matter if the recipient is a long distance provider or an automated system; post-cut-through numbers signal the recipient and therefore should not be considered call-identification information.

In effect CALEA creates a binary division between call "content" and "call-identifying information." The two terms are mutually exclusive of one another. Physically, this division can be seen when looking at a common letter, the address on the envelope is independent from the contents of the letter inside the envelope. The same is true of a telephone communication, except that the content comes after the directional information, instead of inside the envelope. Call content "includes any information concerning the substance, purport, or meaning of that communication." Since post-cut-through numbers communicate the "substance, purport, or meaning" of the call when a subject dials an automated service or a paging system, they are call content and not call-identifying information.

An additional physical example that may be quite helpful in seeing why post-cut-through numbers are not call-identifying information. Consider the difference between the rules for wiretapping and pen registers in the context of the postal service. Assume that the postal service was simultaneously subject to two different rules that coincide with the rule for wiretapping and pen registers. Under the wiretap rule, a law enforcement agency could have the postal service intercept an entire package sent from a particular individual and have it delivered to the law enforcement agency. Using the pen register rule, the law enforcement agency could have the postal service copy the address of a package and deliver this information to the law enforcement agency. Now, assume that the law enforcement agency had received a warrant under the pen register rule, so that the postal service was required to inform it of the destination of any mail sent by a particular individual. If that individual were to send a package to a second individual, and inside the initial package there was a pre-addressed secondary package that the second individual was to send to a third

132. See id.
party, the postal service would have no reason to know that the contents of the package were really destined for the third party and not the second. Furthermore, it would be unreasonable to order the postal service to open each package and check to see whether there was a secondary destination, especially when the law enforcement agency could obtain the entire package under the wiretap rule.

2. Post-Cut-Through Numbers Are Not Reasonably Available

Law enforcement agencies are not authorized by CALEA to require telephone carriers to provide all call-identification information regardless of the availability of the information. Telephone carriers are only required to isolate call-identification information if it is "reasonably available" to the carrier. Because of the way in which telecommunications systems are currently set-up and the way they will be set-up in the near future, post-cut-through numbers are not "reasonably available" to the initial carrier.

Although there is no definition of "reasonably available" provided by the Code, the definition of "reasonably achievable" sheds some light on what Congress may have intended. A majority of the elements to be considered when determining whether an item is "reasonably achievable" relate to the cost of the item. Although no firm figures are available, most observers believe that adding the dialed digit extraction feature will be very expensive for telecommunications carriers.

In order to isolate the post-cut-through numbers dialed during a particular telephone call, telecommunications carriers would have to radically alter their existing switching systems resulting in additional costs. Currently, switches detect numbers with a tone receiver, a device that is built into the switch. However, there are not as many tone receivers as

135. Id.
137. Id.
138. See id.
140. See supra notes 14-21 and accompanying text (describing switching systems).
141. See supra notes 16-19 and accompanying text.
channels for simultaneous calls going through the switch. The switches are built in this manner so that once a call is cut-through, the tone receiver used on the first call can be made available for use on another call. Under the new standards, telecommunication carriers would have to install additional tone receivers on all of their switches because in order to effectuate dialed digit extraction the tone receivers would need to be operational during the entire call, not just during the routing of the call. Current switches do not have enough tone receivers to allow them to be connected for an entire call without causing disruption to the system.

In order to understand how telecommunication switches operate, consider an art museum that limits the number of visitors that can be in the museum at the same time. The limited number of people allowed in the museum is analogous to the number of channels in the switch. Instead of tone receivers directing the calls, the museum has employees direct visitors to their desired exhibit at each door to the museum. Instead of connecting a tone receiver to a call for its entirety, assume employees were instructed to follow certain visitors during their entire visit in case the visitor decided to go to another exhibit and needed directions. In order to ensure that when an employee left her door to follow a visitor there was another employee to direct visitors at the door, the museum would need more employees. In the same way, telecommunications companies will be forced to install extra tone receivers if they are forced to monitor calls for post-cut-through numbers with a pen register, because currently there are not enough tone receivers to monitor calls for their entirety but only until they are cut-through. Although closing the door may be an option for the museum, closing a switch is not an option for the telephone industry; if they decide not to install additional tone receivers into their switches, telephone calls would simply go unconnected.

Therefore to comply with the dialed digit extraction requirements, telecommunications carries would need to undertake a massive upgrade of their existing switching system to

142. See supra note 21 and accompanying text. For example assume that a switch could connect 50 different calls through it at any given time. That switch may only have 5 to 10 tone receivers.
143. See supra notes 19-21 and accompanying text.
144. See May TIA Petition, supra note 16, at 44-45.
145. See id.
include the additional tone receivers. The cost of such an upgrade is estimated to range in the billions of dollars. Over 20,000 switches of differing ages, some dating back to the early 1900s, will need to be modified to have extra tone receivers installed.\textsuperscript{146} Adding further to the cost, each modification will be different as older switches operate much differently than modern switches.\textsuperscript{147} Furthermore, the installation of these capabilities into network switches will most likely occur outside of the normal upgrade cycle\textsuperscript{148} and installing these capabilities out-of-cycle will greatly increase the cost because extra personnel will need to be hired as current personnel will continue to be modifying switches on their normal upgrade cycle.\textsuperscript{149}

In addition to a lack of tone receivers, further advances in technology will make it even more difficult to detect post-cut-through numbers. For instance, voice-recognition dialing allows an individual to speak the name of the person whom she is calling instead of dialing the numbers.\textsuperscript{150} In order for the initial local carrier to determine if an individual had used such a feature after being connected, the local carrier would need to "directly integrate its network intercept facilities with the equipment or databases of the second carrier, or possibly to install voice-recognition hardware and software in its own switches."\textsuperscript{151} In addition, all of the systems would need to be standardized so that they operated in the same way.\textsuperscript{152} Integrating these systems would be prohibitively expensive.\textsuperscript{153}

The definition of reasonably achievable also takes into consideration the "privacy and security of communications not authorized to be intercepted"\textsuperscript{154} and the "policy of the United States to encourage the provision of new technologies and

\textsuperscript{146} See ELECTRONIC SURVEILLANCE, supra note 41, at 38.
\textsuperscript{147} See id.
\textsuperscript{148} See Eric W. DeSilva et. al., Comments of the Personal Communications Indus. Assoc. at 12 (No. 97-213) (Dec. 14, 1998) [hereinafter December PCIA Petition]. On a periodic basis telephone carriers update the technology in all of their switches. See id. Upgrades are made when it is no more expensive to upgrade the switch than to continue using it. See id. By mandating that all switches be modified to meet the new rules, the FCC is forcing telephone carriers to modify their switches when it is more efficient to continue to operate them. See id.
\textsuperscript{149} See id.
\textsuperscript{150} See id. at 45.
\textsuperscript{151} Id.
\textsuperscript{152} See id.
\textsuperscript{153} See id.
DIALED DIGIT EXTRACTION

DIALED DIGIT EXTRACTION runs counter to both of these goals. First, by providing law enforcement agencies with post-cut-through numbers, dialed digit extraction is giving them information that they are not authorized to obtain. Secondly, these capabilities hamper the development of new technologies by diverting resources that could be used for research and development, or installation of new technology to pay for the installation of additional tone receivers, which will provide no additional services to consumers.

3. The Inclusion of Dialed Digit Extraction Violates the Requirements of 47 U.S.C. § 1006(b)

In addition to the issues raised above, the FCC is specifically prohibited from including dialed digit extraction in the technical standard. Section 1006(b) of Title 47 establishes a framework for the FCC to set the technical standards for CALEA. Requiring dialed digit extraction is contrary to this framework because of the costs it will entail and the potential loss of privacy it poses to the public.

Minimizing costs is central to several of the framework's guidelines. The first and third guidelines specifically refer to minimizing costs, while the fourth guideline directs the FCC to issue technical standards that encourage new technologies and services. As discussed earlier, dialed digit extraction will be very expensive, and these costs will be passed along to consumers. There are several reasons for the high costs for implementation. First, not only will existing technologies need to be redesigned to comply with the new standards, but new

155. Id. § 1006(b)(1)(G).
156. See supra notes 123-33 and accompanying text.
158. See id.
159. See id. § 1006(b)(1)-(5).
160. See id. § 1006(b)(1), (3).
161. See supra notes 139-40, 148-53 and accompanying text.
162. See December PCIA Petition, supra note 148, at 12. Congress initially allocated $500 million dollars to subsidize telecommunications companies. See Barbara J. Kern, Ameritech's Comments on the Further Notice of Proposed Rulemaking to establish Technical Requirements and Standards for CALEA at 4 (No. 97-213) (Dec. 24, 1998) [hereinafter Ameritech Petition]. This figure falls drastically short of the over $2 billion that it will cost just to implement the J-STD-025 standards. See December PCIA Petition, supra note 148, at 11. The cost difference will be passed along to consumers in the form of higher rates. See id. at 12.
emerging technology will also need to be redesigned.\textsuperscript{163} Redesigning technology just before it is introduced will drive up the cost of technology and delay implementation.\textsuperscript{164} Second, the short period of time to accomplish compliance will also present problems because telecommunications companies will be strapped to find qualified individuals to perform the necessary work to make their systems CALEA-compliant while at the same time ensuring system reliability.\textsuperscript{165} Telecommunications companies will be forced to hire more personnel and spend additional resources on training new personnel to implement the new standards.\textsuperscript{166} All of these expenses will effect whether or not telecommunications companies are able to offer new services and technologies because increasing the cost of providing new services decreases the likelihood that they will become available.\textsuperscript{167}

In addition, dialed digit extraction does not "protect the privacy and security of communications not authorized to be intercepted" and thus violates the second guideline.\textsuperscript{168} While some of the post-cut-through numbers are secondary phone numbers, other post-cut-through numbers access automated systems and are not authorized to be intercepted.\textsuperscript{169} Telecommunications carriers are not able to differentiate between the different types of post-cut-through numbers.\textsuperscript{170} Dialed digit extraction will therefore provide law enforcement agencies with post-cut-through numbers that represent responses to automated systems. Since law enforcement agencies are only authorized to obtain phone numbers when they have a pen register warrant,\textsuperscript{171} they will be violating the privacy of communications they do not have the authority to intercept.

\textsuperscript{163} See May TIA Petition, \textit{supra} note 16, at 44-45.
\textsuperscript{164} See \textit{id}.
\textsuperscript{165} See December PCIA Petition, \textit{supra} note 148, at 12.
\textsuperscript{166} See \textit{id}.
\textsuperscript{167} See \textit{id} at 14-15.
\textsuperscript{169} See \textit{supra} notes 123-33 and accompanying text.
\textsuperscript{170} See Ameritech Petition, \textit{supra} note 162, at 11.
\textsuperscript{171} See \textit{supra} notes 123-33 and accompanying text.
B. DIALED DIGIT EXTRACTION VIOLATES THE FOURTH AMENDMENT

While the Supreme Court has held that the unauthorized use of a Title III wiretap violates the Fourth Amendment, there is no Fourth Amendment violation for unauthorized use of a pen register. However, the expansion of a pen register to include dialed digit extraction alters this analysis because it expands the type and amount of information that a pen register obtains. Pen registers with dialed digit extraction capabilities should receive the same treatment as Title III wiretaps do under the Fourth Amendment.

The Court has previously held that the Fourth Amendment applies when there is a "legitimate expectation of privacy." Determining if there is a "legitimate expectation of privacy" involves a two prong test: the first prong looks at the subjective expectation of the individual targeted for electronic surveillance. The second prong looks at whether or not society recognizes that individual's subjective expectation of privacy. Obtaining post-cut-through numbers with a pen register violates both prongs of the test. While individuals may not have a subjective expectation of privacy in the numbers that they dial, they most likely do have such an expectation when it comes to content transmitted over the telephone line in the form of post-cut-through digits. There is no functional difference, in terms of expectations, between an individual who calls a bank and speaks to an actual banker to get his balance or an individual who calls a bank and uses an automated system to get his balance. Either way, the individuals are transmitting information over the telephone wire that they do not wish to expose to the public. The type of information typically transmitted over the telephone by use of post-cut-through numbers is incredibly far-reaching: bank account numbers and codes, prescription

172. See supra notes 105-14 and accompanying text.
173. See supra notes 115-21 and accompanying text.
174. See supra notes 123-31 and accompanying text.
175. See supra notes 105-21 and accompanying text.
176. See supra note 116 and accompanying text. The first prong looks at the subjective expectation of privacy of the individual subject to the pen register. See Smith v. Maryland, 442 U.S. 735, 740 (1979). The second prong compares that subjective expectation of privacy against what society is ready to recognize as reasonable. See id.
177. See Third Report, supra note 3, ¶ 123. A typical individual would not freely disclose this type of information.
identification numbers, paging messages, social security numbers, driver license numbers, airline flight information, credit card numbers, voicemail passwords, general account passwords, and responses to automated systems. In *Smith v. Maryland*, the Court noted that individuals know or should know that the numbers dialed to connect a call are made into a permanent record. Accordingly, an individual has no expectation of privacy in the numbers dialed. However, post-cut-through numbers present a different issue. These numbers do not appear on the monthly bill, nor are they documented on a permanent record. Thus, while individuals may knowingly expose the telephone numbers they dial to make telephone call, they may still wish to keep information communicated via post-cut-through numbers private, a subjective expectation of privacy that warrants Fourth Amendment protection.

Furthermore, the subjective expectation of privacy is one that society recognizes as reasonable. In the past, information carried in post-cut-through numbers was transmitted via voice communications over telephone systems. For instance, the information now dialed into a telephone to transfer money from one bank account to another used to be done by talking to a banker instead of using an automated system. The different method of communication does not change the type of information that is transmitted, nor should it change the type of protection that it receives. This information has generally been viewed as protected by the Fourth Amendment and should continue to be so protected.

### III. ALTERNATIVES TO DIALED DIGIT EXTRACTION THAT DO NOT POSE LEGISLATIVE AUTHORITY OR CONSTITUTIONAL PROBLEMS

There are three alternatives that have been proposed by the telecommunications industry to meet the demands of the law enforcement community. Two of these alternatives provide law enforcement agencies with post-cut-through numbers dialed through a secondary provider without reaching beyond

178. *See Smith*, 442 U.S. at 742. The Court noted that individuals see a list of all long distance numbers that they have dialed on their monthly phone bill. *See id.* With mobile telephones, most users see a listing of all numbers that they dial on their bill.

179. *See id.* at 742-43.


CALEA or violating the Fourth Amendment. The third alternative reduces the cost of compliance for telecommunication companies, but presents significant constitutional problems.

First, law enforcement agencies could obtain a Title III wiretap when they are concerned about the possibility of the subject dialing through an 800 number. Obtaining a Title III wiretap would allow law enforcement agencies to record the entire conversation, including post-cut-through numbers. With this information, the law enforcement agency will be able to decipher the post-cut-through numbers and identify the final telephone number that was dialed.

Law enforcement agencies may argue that this alternative will eliminate their ability to conduct pen register wiretaps. Because the requirements for obtaining a Title III wiretap are substantially higher than those to secure a pen register warrant, this alternative prohibits law enforcement agencies from obtaining post-cut-through numbers in instances where the law enforcement agency has enough information to obtain a pen register but not enough to obtain a Title III wiretap. Although these concerns may be relevant, they overlook the fact that the current rules ignore the statutory language of CALEA and invade the privacy of individuals. Law enforcement agencies should not be making policy decisions because Congress has already defined the limits of what law enforcement agencies are allowed to do in terms of conducting wiretaps and pen registers.

Second, law enforcement agencies could serve long distance 800 carriers with pen register warrants in addition to the initial carrier. The post-cut-through numbers for the initial carrier are call-identifying numbers for the long distance carrier. Those numbers inform the long distance carrier how to direct the call. By obtaining a pen register warrant and serving it upon both the initial local carrier and the long distance carrier, the law enforcement agency would be informed of the final number dialed and the path that the subject took to dial that number. This seems to be exactly what Congress had in mind when it passed CALEA since the legislative history in-

---

182. See supra Part I.C.
183. See supra Part II.
184. See supra Part I.B.
185. See supra Part II.A.1.
186. See supra Part II.A.1.
indicates that CALEA was not intended to provide "one-stop shopping."\textsuperscript{187}

Law enforcement agencies may argue that this alternative allows criminals to defeat pen registers by frequently changing the 800 number that they use. This problem could be dealt with in one of two ways. First, long distance providers could be required to keep records of all calls made through their system for a certain period of time. Law enforcement agencies could then subpoena those records when a call was made through that provider. Alternatively, long distance providers could be required to participate in a national network that would gather information from each provider to be made available to law enforcement agencies. With this method, law enforcement would only have to serve two warrants, one on the initial local carrier and one on the national network.

A third alternative is to provide law enforcement agencies with the content of all calls when the law enforcement agency has obtained a pen register warrant. The law enforcement agency would then be required to install the necessary equipment to extract the post-cut-through numbers. This would avoid the need to install extra tone receivers in the telecommunications switches and avoid the expense of developing the dialed digit extraction feature. The device used by law enforcement would be similar to a device currently used to decipher what number have been dialed from the different tones.

However, while this alternative shifts the cost of extracting the post-cut-through numbers from the telecommunications companies to law enforcement agencies and reduces the cost by eliminating the need to install extra tone receivers,\textsuperscript{188} it still requires delivery of the content of telephone calls to law enforcement agencies without a Title III wiretap warrant. This would have constitutional implications because law enforcement agencies would be conducting a "search and seizure" without meeting the requirements of the Fourth Amendment. Law enforcement agencies would have the responsibility to make sure that no one accessed the content of the conversation. They alone would be responsible for limiting their use of the information and not accessing the information contained in the post-cut-through numbers. Given the fact that law enforcement

\textsuperscript{187} H.R. REP. NO. 103-827, at 23 (1994) ("The bill is not intended to guarantee 'one-stop shopping' for law enforcement.").

\textsuperscript{188} See Ameritch Petition, supra note 162, at 12-13.
agencies would possess post-cut-through numbers that repre-
sent content and the probability that they would be tempted to
access this content, this alternative would potentially create
more problems than solutions.

CONCLUSION

As argued by this Note, the inclusion of dialed digit extrac-
tion should be invalidated for a number of reasons. Dialed digit
extraction violates three specific provision of CALEA. Post-cut-
through numbers are not call-identifying information nor are
they reasonably available to the initial carrier. Additionally,
including dialed digit extraction breaches the framework es-
established for technical standards in 47 U.S.C. § 1006(b). Re-
quiring telecommunication carriers to provide law enforcement
agencies with dialed digit extraction overreaches the authority
that Congress gave to the FCC in CALEA.

In addition to its statutory problems, the inclusion of di-
aled digit extraction poses substantial constitutional issues.
The Supreme Court's previous decisions on the constitu-
ality of pen registers are no longer applicable because those deci-
sions assumed that pen registers did not have the capability to
record post-cut-through numbers. Pen registers are now capa-
ble of obtaining the type of information that was traditionally
protected by the Fourth Amendment. However, because pen
register warrants can be issued without meeting the strict re-
quirements of the Fourth Amendment, the inclusion of dialed
digit extraction as a part of a pen register warrant is unconsti-
tutional.

Although the needs of the law enforcement community
should be considered when developing the standards under
CALEA, those needs should not be given priority over other
concerns. Alternatives such as obtaining a Title III wiretap or
serving pen register warrants on secondary carriers will pro-
vide law enforcement agencies with the information that they
need within the statute and without violating the Constitution.