Criminal Division

Statement of
Ms. Laura H. Parsky
Deputy Assistant Attorney General Criminal Division, U.S. Department of Justice

Before the U.S. House of Representatives, Committee on Energy and Commerce
Subcommittee on Telecommunications and the Internet

"Electronic Surveillance in the Digital Age"
September 8, 2004

I. Introduction

Good morning, Chairman Upton, Ranking member Markey, and Members of the Subcommittee. The Department of Justice appreciates the opportunity to address you today on this important subject. As we all are aware, the "Digital Age" in which we now live is offering and will continue to offer tremendous opportunities in telecommunications for both consumers and businesses. The use of high-speed Internet access services is growing rapidly in the United States. In fact, at least one recent report indicates that, for the first time, more U.S. households now connect to the Internet through cable, DSL, and other means of broadband access than through traditional dial-up service. Also, more and more traditional telephone companies, cable companies, and others are offering some means of broadband telephony using Voice over Internet Protocol (VoIP), attracting more and more consumers every day. It is widely believed that such services will essentially replace traditional telephone service in the United States in the not-so-distant future.

The Administration fully supports the rapid and widespread deployment of these communications technologies, understanding that they promise to contribute to increased American productivity and to offer the convenience of reasonably-priced, high-quality service with a variety of useful new features for consumers. Moreover, we welcome and applaud your efforts and the efforts of others in Congress as you carefully debate the proper regulatory environment for new communications technologies. We recognize that we are rapidly expanding into a new and promising world of communications. To automatically apply old-fashioned and likely outdated principles to a new way of doing business is sure to hamper the development of these promising and potent technologies. However, in devising new principles for governing new technologies, we must preserve those safeguards that are critical to our national security and public safety.

The core issue here is responsibility -- responsible government and responsible citizenship. By re-evaluating traditional regulation of communications systems, the government is acting responsibly. Likewise, those who develop and provide such communications services must also assume responsibility. The Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. 1001, et. seq., was drafted ten years ago when Congress could not have anticipated the details of today's communications revolution. However, Congress did have the foresight to predict that such a communications revolution would take place. CALEA requires that, as new technologies are developed, providers act responsibly by engineering their systems in a way that allows law enforcement to execute court-ordered electronic surveillance. As communications technology has progressed, some carriers have never questioned their legal obligations under CALEA or their corporate obligations to act responsibly where public safety and national security are at risk. For each and every carrier in this category, we recognize and applaud their leadership and responsibility. Unfortunately,

however, there are also some carriers who have deployed their technologies without regard to law enforcement's ability to execute court-ordered electronic surveillance and without regard to their corporate responsibility where public safety and national security are at risk. Because of the existence of carriers in this latter category, we have been forced to petition the Federal Communications Commission (FCC) to affirm the legal obligations of carriers to comply with CALEA and to meet non-compliance with robust enforcement actions.

CALEA's obligations are even more important today than they were when the statute was enacted ten years ago. While many carriers act responsibly and in the public interest without the need for compulsory process, there will always be some businesses that will choose to operate without regard to such concerns. Because savvy criminals and terrorists seek out those businesses, we must take steps to eliminate the vulnerability in our national security and public safety created by those businesses. CALEA and the robust enforcement of CALEA will help accomplish this critical goal.

II. CALEA is Critical to Ensuring that Federal, State, and Local Authorities Can Carry Out the Court-Ordered Electronic Surveillance That is Essential to Thwarting the Activities of Terrorists and Other Significant Criminals.

CALEA applies to all telecommunications carriers, a term that is specifically defined in the CALEA statute and that is distinct from and more expansive than the term "telecommunications carrier" used in the Communications Act of 1934, 47 U.S.C. 151 et seq. CALEA requires telecommunications carriers to be able to execute court-ordered wiretaps by isolating and providing to the government, in real-time, the pertinent communications. Carriers also must have the ability to isolate and provide reasonably available call-identifying information, such as numbers dialed, that is the subject of a pen register or other court order. New systems and services thus should be developed and deployed, not in a vacuum, but with recognition of law enforcement's legitimate electronic surveillance needs.

CALEA itself does not authorize wiretaps or pen registers. That authority and the requirements for obtaining the relevant court orders are set forth in other statutes. What CALEA does is to help ensure that, as new telecommunications technologies are developed, carriers using those technologies are capable of isolating and providing to the government communications and related information as required by court orders.

When enacting CALEA in 1994, Congress "concluded that there is sufficient evidence justifying legislative action that new and emerging telecommunications technologies pose problems for law enforcement." H.R. Rep. No. 103-827, at. 14. At that time, Congress was especially cognizant of intercept problems associated with the burgeoning wireless industry and the development of custom calling features. Congress, however, anticipated that future technologies would pose similar problems and thus stated that the purpose of the statute "is to preserve the government's ability,

pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies . . . or features and services . . . while protecting the privacy of communications and without impeding the introduction of new technologies, features and services." Id. at 13.

III. Electronic Surveillance is a Critical Law Enforcement Tool.

It is, of course, no secret that today's criminals use ordinary telephones, cellular telephones, pagers, and the Internet, among other communications devices, in order to coordinate their illicit activities. In investigating terrorism, espionage, and other serious crimes, electronic surveillance is not only one of the most effective tools government has, but often it is the only effective tool. Often criminal organizers and kingpins keep their distance from the criminal conduct they direct through the use of modern communication tools.

There can be no doubt that electronic surveillance takes dangerous criminals off the streets by providing evidence that law enforcement could not have obtained any other way. In fact, one of the requirements for obtaining a federal wiretap order is demonstrating that normal investigative techniques have been or are likely to be inadequate or are too dangerous. Last year alone, 3,674 people were arrested based on evidence obtained through federal and state law enforcement wiretaps. Over the past ten years, over 54,000 people have been arrested based on wiretap evidence. That is as many as 54,000 criminals that might have escaped justice had it not been technologically possible to carry out court-ordered electronic surveillance.

For instance, in a 2002 investigation into members of the Lucchese crime family in New York, wiretaps on cellular telephones and pagers were instrumental in identifying and obtaining convictions of approximately 35 defendants, including three members of the Bonanno crime family. The types of crimes discussed over the wiretapped phones included witness tampering, cocaine distribution, extortion and violence in aid of racketeering, loansharking, and illegal gambling.

In a recent investigation of a marijuana distribution network operating in New York, an intercepted call over a wiretapped phone alerted police to a robbery and double homicide which had just occurred in the Bronx. That valuable evidence allowed authorities to arrest three individuals within hours of the homicides. Investigators later established that several individuals had attempted to rob the targeted marijuana sellers. During the attempted robbery, two individuals were killed by gunshot wounds and a third was shot in the chest and survived. The wiretap evidence helped police piece together the events that had occurred and also helped establish narcotics trafficking charges against additional defendants.

Electronic surveillance is also critical to identifying and ultimately dismantling organized criminal networks, including major national and international drug cartels. Last year, a wiretap in Georgia led to seizures of tons of illegal drugs and millions of

dollars. Another wiretap investigation led to over one hundred arrests in the United States and abroad and numerous U.S. prosecutions, as law enforcement dismantled an international drug distribution ring responsible for bringing large quantities of heroin and cocaine into the United States from Colombia. Electronic surveillance has allowed us to take cocaine, heroin, methamphetamine, and many other dangerous drugs off our streets and away from our children.

While electronic surveillance remains vital to investigating scourges such as organized crime and drug trafficking, against which we continue to fight, it is even more important to the Department's highest priority -- fighting the war on terrorism. The cell structure and worldwide scope of modern terrorist groups make electronic surveillance essential to uncovering these lethal networks before they strike us in ever more devastating ways. In one recent terrorism investigation, three defendants were charged with providing material support to terrorists as well as solicitation of terrorist crimes of violence, including kidnapping and murder. Virtually all of the evidence against these three defendants consists of audio recordings and fax transmissions obtained through wiretaps and listening devices.

Electronic surveillance consistently helps authorities prevent crimes and save lives. In a recent child sexual exploitation investigation in Oklahoma, investigators obtained judicial authorization to intercept all wire communications of a pimp who traveled interstate in order to sell children for sexual activity. The pimp was recorded talking about grooming children to become prostitutes, physically beating his victims into compliance, and marketing the children as prostitutes in numerous states. Further, the electronic surveillance helped identify a national child prostitution network and generated investigations in other states. To date, the United States Attorney's Office in Oklahoma City has federally charged nine defendants for sexually exploiting children, and more indictments are pending. Significant state charges have also been filed against ten perpetrators of these horrible crimes. Already, three children (one from Las Vegas, one from New Mexico, and one from Oklahoma) have been rescued by law enforcement thanks to the electronic surveillance. Moreover, probably thousands of physical and sexual assaults upon children have been prevented as a result of these prosecutions that were dependent upon electronic surveillance.

In a narcotics-related wiretap investigation in the New Orleans area, the target of the investigation discussed arrangements for a heroin transaction with traffickers from New York. In subsequent intercepted conversations, the target told his narcotics associate that he intended to kill the New York suppliers after they delivered the heroin. Based upon this information, law enforcement quickly arrested the New York suppliers and thwarted their intended murder. The New Orleans target was then arrested, pleaded guilty, and was ultimately sentenced to life in prison.

In another case, wiretaps used to investigate a violent Russian brigade helped to develop evidence of the organization's involvement in armed robberies, extortion, and arson, among other crimes. Calls intercepted during the investigation uncovered plans

for a violent kidnapping-for-ransom scheme. The wiretap evidence allowed law enforcement to quickly make the arrests necessary to prevent the kidnapping.

IV. In the Absence of Compliance With CALEA, Technological Constraints Can Prevent or Hinder Wiretaps, Allowing Criminals to Exploit Perceived Technological Gaps to Avoid Interception.

As critical as electronic surveillance is to the investigation of many serious crimes, it is becoming technologically more difficult to carry out wiretap orders and, for some state and local authorities, sometimes impossible to do so. There have been occasions where, because of technological gaps with respect to certain services, telecommunications carriers were unable to provide, or were unable to provide in usable form, the content of communications or related information as required by court orders.

Simply put, the equipment needed to carry out an intercept order or pen register has become more sophisticated as telecommunications technology has advanced. Today's digitized communications are provided by many different companies who use many different protocols and transmit communications over many different wires and cables and over a myriad of frequencies through the air – even during a single call. CALEA therefore requires that telecommunications carriers and their equipment vendors work together in designing new technology so that court-ordered interception is technologically possible.

CALEA's provisions are critical to ensuring public safety and national security. Criminals know that electronic surveillance is an extremely effective law enforcement tool, and they have always gone to great lengths to avoid it. Their tactics have included the use of numerous communication devices in order to isolate the damage done if a particular device is compromised and, most relevant to CALEA, the quick migration to particular technologies that they suspect law enforcement will have difficulty intercepting. Criminals and terrorists certainly do not want to be caught, and they are quick to take advantage of any perceived gap in our ability to detect and disrupt their criminal activities.

V. The FCC is Carefully Considering the Application of CALEA to Advanced Telecommunications Technologies.

In the face of the real and growing threat to public safety and national security posed by the misuse of VoIP and other new telecommunications technologies, the Department of Justice has petitioned the FCC to issue a rulemaking with respect to the application of CALEA to advanced communications technologies such as broadband Internet access and certain forms of broadband telephony. This subcommittee hearing comes in the midst of the FCC's consideration of the Department's petition and the resulting, vibrant discourse involving the Department, other law enforcement entities,

industry, and special interest groups.

In our petition for expedited rulemaking, filed last March, we requested that the Commission rule that CALEA applies to broadband internet access services and certain forms of broadband telephony services; reaffirm that the push-to-talk services now offered by many cellular telephone companies are subject to CALEA; identify the packet-mode services covered by a CALEA implementation Order issued in 1999 and establish compliance deadlines with respect to that Order; adopt rules for expeditiously determining whether a new technology is subject to CALEA and for establishing compliance deadlines and administrative enforcement procedures for non-compliance; and resolve cost recovery issues.

It is important to make clear that through this petition to the FCC, the Department is not asking for expansion of CALEA; that is something only Congress is empowered to do. Rather, we have asked the Commission, pursuant to its mandate, to interpret and implement CALEA in light of emerging telecommunications technologies and an apparent confusion among some service providers and sectors of the telecommunications industry concerning their CALEA obligations.

In crafting CALEA, Congress wisely did not limit its scope to one particular technology, service, or suite of features, but rather set in place a structure that anticipated and provided for a vast array of technological advances. As the then Director of the FBI testified in support of the legislation, CALEA was

> intended to stand the test of time . . . . It is specifically designed to deal intelligently and comprehensively with current and emerging telecommunications technologies and to preclude the need for much more restrictive and more costly legislation in five or ten years when court-authorized interceptions would no longer be possible due to further technology advances.

Hearing on Police Access to Advanced Communications Systems Before the Senate Subcommittee on Technology and the Law of the Committee on the Judiciary and the House Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary (statement of Louis J. Freeh, Director of the Federal Bureau of Investigation). Thus, Congress has already recognized the importance of ensuring that, as advanced communications technologies develop, industry develops the technical means to implement court orders.

In response to the Department's petition, dozens of state and local law enforcement entities and associations filed comments with the FCC emphasizing the critical need to preserve CALEA. State and local entities conduct annually almost three-fifths of all wiretaps in the United States. As articulately expressed by the

National Association of District Attorneys:

> For over a decade we have been pleading for the tools and the laws we need to protect the people in our communities. We will never know whether we could have prevented the tragic consequences of September 11th had we had the investigative tools we have been asking for since 1992. We only know that we will need every advantage to prevent such a tragedy from ever occurring again.

Comments of the National Association of District Attorneys, In the Matter of Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act, FCC 04-187, at 2.

Moreover, many of the responsible members of the communications industry have agreed with law enforcement, through comments filed in other related proceedings, that carriers play an important role in protecting public safety and national security. One industry association put it simply: "American citizens should be assured that communications companies are providing appropriate help to law enforcement." Comments of the United States Telecommunications Association, In the Matter of IP-Enabled Services: Notice of Proposed Rulemaking, FCC 04-28, at 36-37.

VI. In Its Recent NPRM, the FCC Has Recognized the Importance of CALEA in The Context of Emerging Advanced Technologies.

Last month, after receiving extensive comments on the Department's petition, the FCC unanimously issued a Notice of Proposed Rulemaking and Declaratory Ruling concerning a wide variety of CALEA issues ("CALEA NPRM"). The CALEA NPRM states unequivocally that "it is the Commission's primary policy goal to ensure that [law enforcement agencies] have all of the resources that CALEA authorizes to combat crime and support Homeland Security," and it recognizes the need to balance that interest with the competing privacy and technology development interests. CALEA NPRM at ¶4. While the Department is still analyzing this lengthy issuance and will soon provide formal comments to the FCC, a few things are important to highlight. The CALEA NPRM tentatively concludes that CALEA applies to such services as facilities-based broadband Internet services and managed VoIP telephone services, seeking comment on the FCC's legal reasoning to support such conclusions. In addition, the Commission issued a declaratory ruling that wireless push-to-talk services are subject to CALEA. Although the Commission did not agree with the Department on every point raised in our petition, we are pleased with the seriousness with which the Commission is approaching these critical issues.

Further, in the CALEA NPRM, the FCC recognized that law enforcement does

not seek the power to dictate how the Internet should be engineered or the power to veto the deployment of new telecommunications services. Law enforcement cannot – nor do we seek to – dictate to any carrier how best to design its service or what services it can or cannot offer. We only ask that any service comply with the law in order not to imperil public safety and national security. In light of the fact that CALEA solutions can be just as innovative as the services themselves, the FCC appropriately committed itself to "finding solutions that will allow carriers and manufacturers to find innovative ways to meet the needs of the law enforcement community without adversely affecting the dynamic telecommunications industry." CALEA NPRM at ¶ 31.

It is worth noting that nothing in the CALEA NPRM precludes the FCC from making an independent assessment of whether a carrier is subject to other economic regulation under the Communications Act of 1934, as amended. In confining its analysis to CALEA, the Commission explicitly stressed that the CALEA NPRM "in no way predispose[s] how the Commission may proceed with respect to adopting a regulatory framework for Internet Protocol ("IP")-enabled or broadband services or determining their legal classification under the Communications Act." CALEA NPRM at ¶ 1, n. 1.

VII. Several Misconceptions About CALEA and the Department's Efforts to Secure Its Implementation Warrant Clarification.

I'd like to take a few moments to address several misconceptions about CALEA and about the Department's implementation efforts.

A. The Department's Petition Does Not Seek to Erode the Strict Constitutional, Statutory and Regulatory Limitations Imposed on Electronic Surveillance.

While electronic surveillance is a necessary tool, we are mindful that it is also a very powerful tool -- one that has serious implications for the privacy of citizens. Accordingly, law enforcement only uses electronic surveillance as a method of last resort, and even then we adhere to strict limitations on its use.

As I briefly mentioned before, CALEA itself does not authorize electronic surveillance. In presenting our views to the FCC concerning the interpretation of CALEA, the Department is not seeking expanded authority to conduct wiretaps. As Congress said when enacting CALEA, "[s]ince 1968, the law of this nation has authorized law enforcement agencies to conduct wiretaps pursuant to court order. That authority extends to voice, data, fax, e-mail and any other form of electronic communication. The bill will not expand that authority." H.R. Rep. No. 103-827, at 17.

The limitations on law enforcement's use of wiretaps are imposed by the Constitution, statutes, and internal Department procedures. First, the U.S. Constitution

obviously places important parameters on our use of electronic surveillance. Under the Fourth Amendment, the government must demonstrate probable cause to a neutral magistrate before obtaining a warrant for a search, arrest, or other significant intrusion on privacy.

Congress and the courts have also provided statutory limits beyond those required by the Constitution. For instance, law enforcement must obtain a "trap and trace" or "pen register" court order to obtain information identifying who is receiving or sending communications to or from a particular suspect, even though not required under the Constitution. *See* 18 U.S.C. 3121 et. seq.

The statutory authorization for law enforcement wiretaps, 18 U.S.C. §§ 2510-22 (commonly known as "Title III"), as amended by the Electronic Communications Privacy Act (ECPA) in 1986, creates an even higher burden for obtaining the real-time interception of the content of communications. The Senate Report on Title III stated explicitly that the legislation "has as its dual purpose (1) protecting the privacy of wire and oral communications and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized." Senate Committee on the Judiciary, Omnibus Crime Control and Safe Streets Act of 1967, S. Rep. No. 1097, 90th Cong., 2d Sess. (1968) at 66. When Title III was updated in 1986 to include provisions regarding electronic communications, the Senate Report stated that ECPA represented "a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies." Senate Committee on the Judiciary, Electronic Communications Privacy Act of 1986, S. Rep. No. 541, 99th Cong., 2d Sess. (1986) at 5. Accordingly, under Title III, in order to obtain a court order to capture the contents of communications as they occur, the government must show that normal investigative techniques for obtaining information about a serious felony offense have been or are likely to be inadequate or are too dangerous, and that any interception will be conducted so as to ensure that the intrusion is minimized.

Even beyond the limits placed by the Constitution and the Congress, the Department of Justice has its own internal procedures to provide still more safeguards. For example, the Office of Enforcement Operations (OEO) in the Criminal Division of the Department reviews proposed Title III applications to ensure that the request for interception satisfies the protections of the Fourth Amendment and complies with applicable statutes and regulations. Even if OEO recommends authorizing a request, the application cannot go to a court without approval by a Deputy Assistant Attorney General or higher-level official in the Department. The fact that not a single application for electronic surveillance under Title III was rejected by a federal court in all of 2003 is a testament to the vigilance and care the Department takes when asking for this authority.

If the Department of Justice approves a federal Title III request, it still must, of course, be submitted to and approved by a court of proper jurisdiction. The court will

evaluate the application under the Fourth Amendment and using the familiar standards of Title III. By statute, for example, the application to the court must show, through sworn affidavit, why the intercept is necessary as opposed to other less-intrusive investigative techniques. The application must also provide additional detail, including whether there have been previous interceptions of communications of the target, the identity of the target (if known), the nature and location of the communications facilities, and a description of the type of communications sought and the offenses to which the communications relate. By statute and internal Department regulation, the interception may last no longer than 30 days without an extension by the court. All intercepted communications are sealed by the court, further protecting privacy.

Often courts also impose their own safeguards. For example, many federal courts require that the investigators provide periodic reports to the court setting forth information such as the number of communications intercepted, the steps taken to minimize irrelevant traffic, and whether the interceptions have provided information relevant to the criminal investigation. The court may, of course, terminate the interception at any time.

It is only after we have complied with these comprehensive regulatory, statutory, and Constitutional protections that CALEA comes into play and ensures that a court order can be implemented. Our recent filings with the FCC do not seek to change any part of this carefully calibrated system.

B. Implementation of CALEA Will Help Protect Privacy.

It is important to make clear that CALEA, itself, actually provides critical protection of privacy rights. The argument that full implementation of CALEA will threaten individual privacy rights is simply misguided. CALEA strikes a delicate balance among three sometimes competing goals: "(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." H.R. Rep. No. 103-827, at 13. As the House of Representatives explained in the report, "the bill further protects privacy by requiring the systems of telecommunications carriers to protect communications not authorized to be intercepted." Id. at 10.

CALEA addresses privacy concerns in two ways. First, it requires that providers be able to separate out the communications involving the equipment, facilities, or services of the particular subscriber whose communications law enforcement has an order to intercept. This provision promotes both efficiency and privacy. Second, CALEA requires that a service provider be able to separate out call-identifying information from the content of communications. This protects the call content from law enforcement access where law enforcement only has legal grounds to obtain the

call-identifying information. CALEA Section 103; 47 U.S.C. 1002. A carrier's compliance with CALEA when implementing a court-ordered wiretap or a pen register order thus protects individuals' privacy rights.

C. In Keeping with the Provisions of CALEA, the Department of Justice Does not Seek to Dictate the Design of Telecommunications Systems.

It is also important to stress that the Department does not seek to dictate the design of new telecommunications systems. In fact, CALEA explicitly prohibits any such undertaking by providing that it "does not authorize any law enforcement agency or officer . . . to require any specific design . . . to be adopted by any provider [or] manufacturer . . . ," and it does not authorize any law enforcement agency or officer "to prohibit the adoption of any equipment, facility, service, or feature by any provider . . . [or] manufacturer." CALEA Section 103, 47 U.S.C. 1002(b)(1).

What the Department does seek is to ensure that new communications services and features to which CALEA applies are deployed with CALEA solutions in place whenever feasible. Indeed, Section 106 of CALEA mandates that carriers consult with manufacturers "as necessary, in a timely fashion" to ensure "that current and planned equipment, facilities, and services comply with [CALEA] capability requirements[.]" 47 U.S.C. 1005 (emphasis added). CALEA solutions may be developed by individual service providers or by industry, but they must be developed. Any amount of time that a terrorist or other dangerous criminal can use a communications service without a capability for court-ordered interception is too long.

D. The Department is Not Seeking to Re-allocate the Costs of CALEA Implementation.

Finally, the Department is not seeking to re-allocate the costs of CALEA implementation to industry or consumers. It is CALEA itself that places any cost burden on telecommunications carriers in the first instance, rather than on the government, for equipment, facilities, and services installed or deployed after January 1, 1995. CALEA Section 109(b); 47 U.S.C. 1008(b). This same provision, however, also allows carriers to seek a determination of whether implementation of a CALEA solution is "reasonably achievable" in light of costs and other issues and allows carriers to seek compensation for costs or reprieve in some circumstances. CALEA recognizes that the greatest cost efficiency can usually be achieved by building intercept solutions into a system's initial design prior to deployment, rather than as a retrofit.

VIII. Conclusion

Now, ten years after the enactment of CALEA, we must not back away from the important principles behind CALEA. If anything, it is even more critical today than in 1994 that advances in communications technology not provide a haven for criminal and terrorist activity. While we recognize the desirability of and need for the development and deployment of advanced telecommunications technologies, we must at the same time act responsibly to preserve the national security and public safety mandates of CALEA. The Department of Justice appreciates this Subcommittee's leadership in seeking to promote new telecommunications technologies in a manner that addresses these national security interests, and we thank you for your continuing support.