Criminal Division

The Testimony of

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

U.S. Senate Committee on Commerce, Science and Transportation
The VOIP Regulatory Freedom Act, S. 2281
Wednesday, June 16, 2004

I. Introduction Good morning Chairman McCain, Ranking Member Hollings, and Members of the Committee. I appreciate the opportunity to testify this morning about telephone service that uses the Internet Protocol ("VoIP"). How you treat this service will profoundly impact the Department of Justice's ability to protect communities across the nation from the harms inflicted by drug trafficking, organized crime, and terrorism and fundamentally to protect the national security of the United States. It is imperative that public safety and national security concerns be carefully considered when evaluating advances in communications technology.

II. VoIP Presents Both Opportunities and Challenges. First, I want the Committee to know that the Department of Justice is keenly aware that telephone service that uses the Internet Protocol has the potential to provide tremendous benefits to the American consumer. We are hopeful that this form of telephone service will cost less, provide better service, and include exciting new features. The Administration has spoken in favor of VoIP in the past, and the Administration continues to support the rollout of new technologies, such as VoIP. As with all new technologies, the Department of Justice celebrates the benefits it promises, while at the same time working vigorously to protect our country and citizens against its misuse.

III. Electronic Surveillance is a Critical Law Enforcement Tool. As part of that work, I am here to underscore how very important it is that this type of telephone service not become a haven for criminals, terrorists, and spies. Access to telephone service, regardless of how it is transmitted, is a highly valuable law enforcement tool. Not only is electronic surveillance one of the most effective tools government has to combat crimes such as terrorism, espionage, and organized crime, but it is often the only effective tool.

Any criminal conspiracy requires communication in order to operate. Today, these communications often do not occur in person, where law enforcement could observe a meeting taking place -- could see people physically coming and going. Instead, criminals do what many of us do, they use the telephone. Telephones allow criminals to coordinate their activities and allow organizers and kingpins to keep their hands clean of the most sordid criminal conduct.

Federal and state prosecutors often note the importance of evidence gathered through electronic surveillance in obtaining arrests and convictions. Last year alone, 3,674 people had been arrested based on evidence obtained through wiretaps. Over the past ten years, over 54,000 people have been arrested based on wiretap evidence. That is up to 54,000 criminals that might have escaped justice had court-ordered electronic surveillance not been available.

Electronic surveillance not only provides otherwise unobtainable evidence of criminal activity, but it also helps the authorities prevent crimes and save lives. For instance, in his 1994 testimony, former Director of the Federal Bureau of Investigation ("FBI"), Louis Freeh, described how electronic surveillance led to prevention of terrorist attacks such as the planned rocket attack against an FBI field office and an attack on a nuclear power facility.

Electronic surveillance is also a critical law enforcement tool to identify and dismantle organized criminal organizations, including major national and international drug cartels. Last year, a wiretap in California led to seizures of literally thousands of tons of illegal drugs and millions of dollars. Another wiretap investigation led to over one hundred arrests, as law enforcement dismantled an international drug distribution ring that was responsible for vast quantities of heroin and cocaine coming into the United States from Columbia through Aruba. Electronic surveillance has allowed us to take cocaine, heroin, methamphetamine, and many other dangerous drugs off our streets and away from our children. Because electronic surveillance is such an effective law enforcement tool, criminals go to great lengths to shield their telephone communications. One tactic they employ is to use a wide array of communication devices, trying to isolate the damage done if a particular means of communicating is compromised. For instance, a recent Drug Enforcement Administration investigation revealed a Miami drug trafficker who is known to have used 20 different cellular phones in a three-month period.

What is more, we know that when it becomes known that law enforcement has difficulty detecting communications over a particular technology, criminals quickly migrate to that technology. While I obviously cannot go into detail on this point, suffice it to say that criminals do not want to be caught, and they are quick to take advantage of any gap in our ability to detect and disrupt their criminal activities.

If criminals could use new technologies to avoid law enforcement detection, they could use these technologies to coordinate terrorist attacks, to distribute drugs throughout the United States, and to pass along national security secrets to our enemies. If the criminals were successful, we would learn about these plots only after terrible damage had been done, or in some cases not at all. Put simply, law enforcement cannot effectively protect the public and enforce the laws in today's world without electronic surveillance.

IV. Because Electronic Surveillance Is Such A Powerful Tool, It Is Rightfully Subject To Equally Powerful Limits On Its Use.

While electronic surveillance is a necessary tool, we are mindful that it is also a very powerful tool, which has serious implications for the privacy of citizens. As such, we only use electronic surveillance as a tool of last resort, and even then we adhere to strict limitations on its use. First, the U.S. Constitution 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 in order to obtain information identifying who is sending or receiving communications to or from a particular suspect, even though not required under the Constitution. See 18 U.S.C. 3121 et. seq. The Wiretap Act, 18 U.S.C. §§ 2510-22 ("Title III"), places an even higher burden on the real-time interception of the content of wire 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. Accordingly, under Title III, in order to obtain a court order to capture 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 each proposed Title III application 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. The remedies for improperly intercepting communications in violation of Title III or the Electronic Communications Privacy Act ("ECPA") can include criminal sanctions, civil liability, and, for law enforcement agents, adverse employment action. For violations of the Fourth Amendment, of course, the remedy of suppression is also available.

All of these requirements and procedures ensure that electronic surveillance is only used when absolutely necessary to detect and prosecute serious criminal violations. It is a tool of last resort reserved for only the worst offenses against our civil society. It is done with the approval and oversight of the courts, and done in ways as narrowly tailored as possible to the investigation of specific individuals for specific criminal conduct. Further, if it is misused, there are serious consequences. V. CALEA is Critical to Implementing Court Orders Authorizing Electronic Surveillance.

While electronic surveillance is a critical tool for law enforcement, it is not always easy to implement, and it is becoming even more difficult. In the past, when law enforcement agencies conducted court-authorized electronic surveillance, they were able to go to one provider and access a "local loop" that allowed a single location for the collection of content and related dialing information for all communications with the subject's telephone number. However, it has been a long time since all that was required to implement a court order for electronic surveillance was a call to Ma Bell and a set of alligator clips. Today, communications are transmitted over many different wires and cables and over a myriad of frequencies through the air. These communications are provided by many different companies who use many different protocols.

Making matters even more difficult, the parties that provide the transmission and switching of these communications may have no relationship with the providers who perform call set-up and addressing functions. It is because of both the breadth of services and the technical complexity of features associated with each one that law enforcement relies on the designers to assist in providing interception capability for the select cases where a court has ordered such interception.

The Congress has already recognized this problem and taken decisive action to prevent public safety and national security from being imperiled as a result of the digital communications revolution. In 1994, Congress "concluded that there is sufficient evidence justifying legislative action that new and emerging telecommunications technologies pose problems for law enforcement." In response, you prudently passed the Communications Assistance for Law Enforcement Act ("CALEA").

In enacting CALEA, you made clear 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 such as digital or wireless transmission modes, or features and services such as call forwarding, speed dialing and conference calling, while protecting the privacy of communications and without impeding the introduction of new technologies, features and services." Thus, CALEA struck a balance among sometimes competing goals. As the legislative history makes clear, "the bill seeks to balance 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."

In crafting this solution, you wisely did not limit CALEA's scope to just 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, it was intended to stand the test of time and overcome the shortcomings of the 1970 amendment. 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. Any legislation that would limit its application to technological impediments on a piecemeal basis would be disastrous. Piecemeal legislation which deals only with current problems or some of the problems would result in common carriers fully deploying new technologies which would impede electronic surveillance and which would cause the government to return to Congress repeatedly.

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) ("Freeh CALEA Testimony"). Thus, Congress has already recognized the importance of ensuring that, as advanced telephone service technologies develop, they must have the technical ability to implement court orders for surveillance. Now, ten years later, we must not back away from the important principles behind CALEA. If anything, it is even more critical today than in 1994 (when CALEA was enacted) that advances in communications technology not provide a haven for criminal activity and an undetectable means of death and destruction.

It is important to be very clear here - we ask today only that you not undermine current capabilities to implement court orders and conduct critical law enforcement activities. CALEA is about the practical necessity of implementing existing lawful authority, not expanding it. Congress said so itself, noting in the legislative history to CALEA that "[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." Nothing in CALEA gives law enforcement the authority to conduct any surveillance. It is only after all of the comprehensive regulatory, statutory, and Constitutional protections described above have been complied with that CALEA comes into play and ensures that the order of the court can be carried out. In fact, CALEA explicitly and intentionally protects privacy in very important ways. As the House of Representatives explained in its report on CALEA, "the bill further protects privacy by requiring the systems of telecommunications carriers to protect communications not authorized to be intercepted." It does this in two ways. First, CALEA requires that providers be able to separate out the communications of just the subscriber for whom law enforcement has an order to intercept communications.

This provision benefits 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. VI. The Application of CALEA to Advanced Telecommunications Technologies Is at Issue in Proceedings Before the Federal Communications Commission. This hearing comes in the midst of a vibrant debate on similar issues at the Federal Communications Commission ("FCC"). The FCC recently issued its Notice of Proposed Rulemaking concerning the appropriate treatment of IP-enabled services, including telephone service that uses the Internet Protocol. Hundreds of parties have submitted their thoughtful consideration of the issue, including the Department of

Justice. With regard to CALEA in particular, the Department of Justice has petitioned the Commission for an expedited rulemaking to clarify which services and entities are subject to CALEA. We expressed our view that broadband access and broadband telephony service providers are "telecommunications carriers" under CALEA, and, therefore, they must be capable of implementing court orders for surveillance.

In both the IP-enabled services and CALEA proceedings at the FCC, the Department of Justice has made the same points that I want to emphasize here this morning: (1) that public safety and national security will be compromised unless court orders for electronic surveillance can be implemented by providers; (2) that assistance requirements should apply to every service provider that provides switching or transmission, regardless of the technologies they employ; and (3) that if any particular technology is singled out for a special exemption from these requirements, that technology will quickly attract criminals and create a hole in law enforcement's ability to protect the public and the national security.

The CALEA proceedings in particular are creating a compelling record regarding the drastic consequences if we were to fail to provide law enforcement the tools it needs to protect public safety. Thus far, dozens of state and local law enforcement entities - from New York to Los Angeles and dozens of places in between - have filed comments at the FCC emphasizing the critical need for these tools and the dire consequences of failure.

It is not surprising that so many police chiefs and district attorneys came out in strong support of the Department in this matter, because state and local governments account for almost three-fifths of all wiretap applications. As the National Association of District Attorneys expressed so well in their comments to the FCC in the CALEA Rulemaking proceeding:

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, RM-10865, at 2. We are also pleased that a number of the Commissioners have already publicly acknowledged the need to preserve law enforcement access to telephone service that uses the Internet Protocol. Chairman Powell was unequivocal in his

statement accompanying the recent IP-Enabled Services Notice of Proposed Rulemaking. He stated:

CALEA requirements can and should apply to VoIP and other IP-enabled service providers, even if these services are "information services" for purposes of the Communications Act. Nothing in today's proceeding should be read to suggest that law enforcement agencies should not have the access to communications infrastructure that they need to protect our nation. On the contrary, all IP-enabled services should consider the needs of law enforcement as they continue to develop innovative technologies.

Statement of Chairman Michael K. Powell, In the Matter of IP-Enabled Services: Notice of Proposed Rulemaking, FCC 04-28. Further, many responsible members of the communications industry have agreed with the Department that their assistance is critical to public safety and national security. One member of the industry 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. There is one aspect of the Department's position in the CALEA proceedings before the FCC that is important to clarify to avoid misunderstanding. 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. CALEA specifically states that it "does not authorize any law enforcement agency or officer to require any specific design . . . ." 47 U.S.C. 1001(b)(1)(A). Nor does CALEA authorize law enforcement "to prohibit the adoption of any equipment, facility, service, or feature . . . ." 47 U.S.C. 1002(b)(1)(B). As law enforcement requested, Congress made the providers' obligations under CALEA generic by design. The then Director of the FBI could not have been more clear on this point, when he testified in support of the CALEA legislation in 1994:

The Government purposely eschewed setting any technical standards because it does not desire to 'dictate' particular technological solutions. It is the Government's position that each common carrier is best positioned and qualified to determine how it will meet the requirements in the most cost-effective way.

Freeh CALEA Testimony. Law enforcement cannot - nor do we seek to – dictate to any carrier how best to design their service or what services they can or cannot offer. We only ask that any service comply with the law in order not to imperil public safety and national security. VII. S. 2281 Could Significantly Diminish the Department of Justice's Ability to Investigate Serious Crimes and Protect the Safety of the American People.

With regard to the bill that is the subject of this hearing, S. 2281, the Department of Justice has a number of comments, all of which we hope to provide formally in writing in the near future. Given the focus of this hearing, however, I will limit my remarks to how the bill could impact CALEA and law enforcement's ability to implement court-ordered electronic surveillance. In this regard, the Department of Justice is concerned that S. 2281 could be read to significantly diminish the Department's ability to investigate serious crimes and protect the safety of the American people. S. 2281 seeks to exempt providers of telephone service that uses the Internet Protocol from many obligations to which other telephone companies are subject. The Department of Justice recognizes that this Committee rightfully must consider whether this type of telephone service may require different regulatory treatment for many purposes, including economic. When considering such regulatory treatment, it is very important to keep in mind how it will impact our CALEA authority and the implications for public safety. Recognizing the importance of law enforcement access to this type of telephone service, the bill would require the Commission to "require a provider of a connected VOIP application to provide access to necessary information to law enforcement agencies[;]" however, the bill restricts the obligation to "not less than that required of information service providers." Two aspects of this provision could result in a diminished or inadequate ability for law enforcement to fulfill court orders for electronic surveillance. A. S. 2281 Only Identifies Assistance Requirements for Providers Who Interconnect with the Publicly Switched Telephone Network.

First, S. 2281 only requires law enforcement's access to "connected VoIP application[s]." The bill defines a "connected VoIP application" as "a VoIP application that is capable of receiving voice communications from or sending voice communications to the public switched telephone network, or both." In other words, the bill protects law enforcement access to those technologies that continue to rely on one particular set of wires, the publicly switched telephone network. As the Congress already recognized when it passed CALEA, limiting law enforcement's ability to obtain assistance from a provider to only a particular type of wires, never mind one that is quickly being overtaken by new innovations, can significantly diminish law enforcement's ability to protect public safety and national security. B. S. 2281 Could Be Read to Limit the Obligation To Provide Government Access To "Not Less Than That Required of Information Service Providers."

Second, and more importantly, the bill would require law enforcement access to necessary information be "not less than that required of information service providers." Although it is unclear what this provision is intended to mean, it runs the risk that it could be interpreted as a ceiling rather than a floor. Currently, CALEA exempts "information services" from its assistance capability requirements. If telephone service providers were to have only the obligations of those entities that are information service

providers under CALEA, then they would be exempt from CALEA and the Department of Justice's ability to investigate serious crimes and protect national security would be undermined. VIII. Conclusion Mr. Chairman, the Department of Justice appreciates your support as we continue with the difficult work of protecting our nation and enforcing our laws during times of rapid technological change. We are concerned that S. 2281 could create a safe haven for criminal activity by not preserving the application of CALEA to new technologies. It is very important that, in taking action regarding telephone service that uses the Internet Protocol, Congress carefully consider implications to public safety and national security. Thank you for the opportunity to testify before you today, and I am happy to answer any questions the Committee may have.