Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of:	)	
Communications Assistance for Law Enforcement Act	)	CC Docket No. 97-213

DECLARATION OF FBI DIRECTOR LOUIS J. FREEH

I, Louis J. Freeh, hereby declare as follows:

1. I am the Director of the Federal Bureau of Investigation (FBI) and have served in this position since September 1, 1993. Prior to being sworn in as the Director, I served as an FBI Special Agent from 1975 to 1981 in the New York City Field Office and at FBI Headquarters in Washington, D.C. In 1981, I joined the United States Attorney's Office for the Southern District of New York as an Assistant U.S. Attorney. I subsequently held positions there as Chief of the Organized Crime Unit, Deputy U.S. Attorney, and Associate U.S. Attorney. In July 1991, I was appointed by President Bush to serve as a United States District Court Judge for the Southern District of New York. I was serving in this position when nominated to be Director of the FBI by President Clinton on July 20, 1993. I was confirmed by the United States Senate on August 6, 1993, and was sworn in as Director on September 1, 1993.

2. The following statements are based on my experience in the field of criminal investigation and prosecution, and on information collected by my staff from sources within

the Federal Bureau of Investigation, state and local law enforcement agencies, and the Administrative Office of the United States Courts. I am making this declaration because of my conviction that court-authorized electronic surveillance of telecommunications[1] is an essential tool for effective law enforcement and that the assistance which the Communications Assistance for Law Enforcement Act (CALEA) requires the telecommunications industry to provide to law enforcement is crucial to our ability to properly utilize this essential investigative tool. I noted many of the following facts in my earlier testimony before Congress, when I spoke in support of the enactment of CALEA. Since then, the telecommunications industry has seen additional advances in technology including the development and deployment of new features and services such as voice dialing and two-way paging, the widespread deployment of Enhanced Special Mobile Radio Services such as "push-to-talk" private network conferencing, and the marketing of digital packet-based services. I can say with even more confidence now than when I testified in 1994 on this matter that, without the effective operation of the assistance capabilities provisions of CALEA, law enforcement will not have the ability to effectively carry out court-authorized electronic surveillance in the face of changes in technology.

3. The nation's telecommunications networks are routinely used in the commission of serious criminal activities, including terrorism, organized crime, drug

---

[1/] Henceforth, as used in this declaration the term "electronic surveillance" refers to court authorized interception of wire or electronic communications obtained through the technique commonly referred to as "wiretapping," as well as acquisition of dialing and signaling information obtained through pen registers and trap and trace devices. Electronic surveillance is a crucial component of the larger family of sophisticated surveillance techniques, which also includes court authorized listening devices for oral communications, consensual monitoring of telephonic and non-telephonic communications and video surveillance devices.

trafficking, violent crime, espionage, fraud and other white collar crime. For this reason, the ability to conduct court-authorized electronic surveillance when these systems are being used to facilitate crimes is an essential tool for effective law enforcement.

4. Congress recognized this fact more than 25 years ago when it passed the Omnibus Crime Control and Safe Streets Act of 1968. Title III of that Act (codified at 18 U.S.C. §§ 2510-2521) contained the first comprehensive federal legislative framework governing electronic surveillance for use in criminal investigations. In passing this legislation, Congress fashioned a comprehensive electronic surveillance framework that carefully balanced the communications security needs and privacy rights of individuals with the needs of law enforcement to fulfill its duty to protect the public and enforce the law. To this end, Congress specified that, above and beyond the traditional requirements of the Fourth Amendment — which include probable cause, the need for impartial review and a warrant, and particularity as to the object of the search — the interception of wire and oral communications would generally be limited to use by law enforcement: (i) only when other investigative techniques have failed, reasonably appear unlikely to succeed, or are too dangerous to attempt, (ii) only for the investigation of serious, statutorily-specified felony offenses, and (iii) only for the interception of criminal communications. The acquisition of non-criminal communications is not authorized, and thus law enforcement is obligated to minimize the interception of such communications. Every application to intercept wire or oral communications must also be reviewed and approved by a statutorily designated

Department of Justice or state official prior to being submitted to the court.[2] It is important to recognize that unless otherwise exempted by statute, for example because one of the parties to a communication has consented to monitoring by law enforcement, Title III surveillance always requires the approval of a court.[3]

5. In light of advances in telecommunications and computer technologies, Congress amended Title III in 1986 by enacting the Electronic Communications Privacy Act (ECPA) to protect electronic communications from unauthorized interception. As with the interception of wire and oral communication, a court order is generally required to intercept electronic communications. The requirements for approval are the same as the requirements for authority to intercept wire or oral communications except that any attorney for the government may approve an application for interception of electronic communications, and such an interception may be conducted in connection with any federal felony, rather than only specifically enumerated felonies. Although the statute provides that any attorney for the government may approve an application for the interception of electronic communications, Department of Justice policy dictates that such applications (with the

---

[2] In 1978, Congress established an analogous federal electronic surveillance regime for use in national security investigations of terrorism, espionage, and intelligence matters: the Foreign Intelligence Surveillance Act of 1978 (FISA) (codified at 50 U.S.C. §§ 1801-1811). Like Title III, FISA requires that orders authorizing electronic surveillance be issued by a federal judge, and many of the other requirements under FISA are the same as for Title III. In addition, FISA requires certification by a Presidential designee that the purpose of the surveillance is to obtain foreign intelligence information, and approval by the Attorney General of each application, prior to its submission to the court.

[3] In certain emergency situations, Title III permits senior Department of Justice or state officials to authorize an intercept prior to obtaining court approval. The intercept must subsequently be approved by a court, or the intercepted communications are treated as having been obtained in violation of Title III.

exception of digital display pagers) be reviewed and approved pursuant to the same process as applications for the interception of wire and oral communications.

6. Portions of ECPA (codified at 18 U.S.C. §§ 3121-3127) also regulate law enforcement's use of "pen registers," which are used to determine the dialing and signaling activity of a facility under surveillance, and "trap and trace" devices, which are used to identify the origin of wire or electronic communications directed to a facility under surveillance. Absent consent, law enforcement must obtain a court order to install either of these devices, which (unlike an order authorizing interceptions under Title III) does not enable law enforcement to intercept the content of communications.[4] Pen registers and trap and trace devices are utilized much more frequently than wiretaps, and the information collected through these less-intrusive means is invaluable in a broad range of investigations. Moreover, pen register and trap and trace information commonly provides a crucial portion of the showing required to obtain a Title III order by providing information that enables law enforcement to identify and link the parties involved in the communications.

7. Court-authorized electronic surveillance is not only an essential investigative tool for federal law enforcement, it is also essential in state and local law enforcement investigations. Forty-five states, Puerto Rico, the United States Virgin Islands, and the District of Columbia have enacted their own electronic surveillance statutes. Approximately fifty-four percent of the criminal-related electronic surveillance of telecommunications

---

[4/] In certain emergency situations, the statute provides that senior Department of Justice or state officials may authorize the installation and use of pen registers and trap and trace devices prior to obtaining court approval. As with emergency Title III authority, subsequent judicial approval must be obtained.

conducted in the United States in 1997 was carried out by state and local law enforcement agencies.

8. Evidence collected by the Administrative Office of the United States Courts indicates that court-authorized Title III electronic surveillance has been conducted sparingly, judiciously, and in compliance with the letter of the law and the spirit of Congress' intent. For example, all of the investigations conducted by federal, state and local law enforcement in 1997 led to the execution of only 1,094 Title III interception orders in that year. Of that number, only 563 orders were for federal investigations; 335 of those orders were executed by the FBI. Well over ninety per cent of the orders issued in 1997 involved the interception of communications on telecommunications networks. The remaining orders authorized the interception of oral communications through listening devices.[5] Between 1987 and 1997, electronic surveillance conducted pursuant to Title III assisted in the conviction of well over 21,000 dangerous felons. As demonstrated by the lives saved and the important investigations and prosecutions successfully completed, the use of electronic surveillance has served the public extremely well.

9. Indeed, law enforcement agencies at all levels of government have uniformly found electronic surveillance to be one of the most important — if not *the* most important — sophisticated investigative tools available to them in the prevention, investigation, and prosecution of many types of serious crimes. This tool has been critical in fighting terrorism, organized crime, kidnaping, drug trafficking, public corruption, fraud, and violent crime, and in saving numerous innocent lives. In many of these cases, the criminal activity under

[5/] These devices are commonly known as "bugs." See footnote 1.

investigation could never have been detected, prevented, investigated, or successfully prosecuted without the use of evidence derived from court-authorized electronic surveillance.

10. Electronic surveillance is not only critical for its value in helping law enforcement prosecute criminals, it is often critical to enable law enforcement to act in time to *prevent* planned criminal activities and the ensuing loss of lives. For example, when the El Rukn gang in Chicago (acting in collaboration with Libya) planned to shoot down a commercial airliner in the United States using a stolen military weapon, electronic surveillance enabled the FBI to prevent this act of terrorism, which would have been on a par with the deadly bombing of Pan Am Flight 103 over Scotland.

11. The El Rukn case is not an isolated incident. In fact, a significant number of violent acts by terrorists, including bombings and murders, have been prevented through electronic surveillance. In 1993, electronic surveillance contributed to the indictment of individuals in the St. Louis-based cell of the Abu Nidal organization on RICO charges including conspiracy to commit murder and conspiracy to bomb the Israeli Embassy in Washington, D.C. In 1990, electronic surveillance assisted law enforcement in preventing foreign-based terrorists from acquiring a Stinger surface-to-air missile that likely would have been used in an attack on civilians, and in another case that same year, also helped law enforcement to prevent several bombings planned by anti-Castro groups based in Miami, Florida.

12. Many violent crimes, including murder, torture, and kidnaping have been successfully prosecuted (and a significant number prevented or curtailed) by law enforcement's use of electronic surveillance:

- In 1990, electronic surveillance of New York City's Green Dragon gang, which got its marching orders via telephone from an individual in the People's Republic of China, disclosed that the gang was about to engage in a shoot out with a rival Asian gang. Acting immediately upon this information, law enforcement arrested sixteen gang members, preventing an imminent violent confrontation and bloodshed.
- In another 1990 case, electronic surveillance assisted in the FBI's successful efforts to thwart two individuals who were conspiring to abduct, torture, and kill a teenage boy for the purpose of making a "snuff murder" film.
- Pen registers and other court-authorized electronic surveillance utilized in the investigation of a New England organized crime family in the early 1980s enabled the FBI to intercept conversations among members of the crime family, wherein the murders of three individuals were planned and details concerning six prior murders were discussed. The FBI was able to prevent two of the three planned murders (but unfortunately was unable to locate the third victim in time to prevent his murder).
- In 1994, law enforcement was able to rescue four kidnaped Chinese nationals as a result of intercepting the telephone conversations of the kidnapers.

13. Kidnaping is an extraordinarily harrowing experience for the victim and his or her family. The use of electronic surveillance, including the consensual surveillance of the victim's family's telephone, is often central to the investigation of kidnapings and the recovery of the victim. In 1997, while executing a Title III order in a drug trafficking investigation, law enforcement discovered through the interception of conversations occurring on a cellular phone that the drug traffickers had kidnaped a Mexican national who

they believed had a large quantity of cocaine. The drug traffickers were threatening to torture the victim by severing his fingers until he told them where they could find the drugs. As law enforcement agents prepared to rescue the victim, they learned through further intercepted conversations that the drug traffickers had locked him in the trunk of their car and were moving him to another location. Because surveillance of these cellular telephone conversations enabled the law enforcement agents to keep pace with this developing situation, they were able to meet the drug traffickers at the second location and rescue the victim before the drug traffickers could carry out their threats.

14. The ability to collect call-identifying information quickly is often particularly critical in kidnaping cases. Kidnaping situations tend to be fast-moving and often involve criminals who are extremely difficult to trace and apprehend. In the kidnaping context, therefore, law enforcement has a particularly strong need to acquire electronic surveillance information rapidly, in order to be able to locate the criminals before they have moved, and to rescue their victims as quickly as possible. The previous example of the Mexican national who was kidnaped and threatened with torture by drug traffickers illustrates the point, as does the 1999 rescue of the 17-year-old son of a prominent Taiwanese real estate investor. On December 15, 1998, kidnapers abducted the teenager from his San Marino, California, home. Two days later, their accomplices in China contacted the boy's father and demanded $1.5 million in ransom. Electronic surveillance enabled law enforcement to track the locations not only of the kidnapers, but also their accomplices in China. On January 4, 1999, as the boy's father delivered $500,000 in ransom to the kidnaper's accomplices, the FBI and other federal, state, and local law enforcement officers raided the California home where the

boy was being held, freed him, and arrested his kidnapers. Officers of China's Ministry of Public Security arrested the kidnaper's accomplices in China.

15. One of the principal purposes for the enactment of Title III in 1968 was to address the great societal threat posed by organized crime. Organized crime is extremely harmful to American business and industry, labor unions, and individuals. Left unchecked, it exerts a choke hold on society, and the subsequent cost — in higher prices for all consumers, underpayment of taxes, reduced output, and lower employment — is estimated to run well into the tens of billions of dollars. With organized crime inevitably comes more violent crime as well, including murder, maiming, and extortion.

16. The vast majority of the FBI's major organized crime investigations have utilized electronic surveillance. Electronic surveillance is particularly essential to the investigation of organized crime figures, because they tend to be sophisticated and extremely cautious. Without electronic surveillance and other advanced investigative techniques, it would be extremely difficult to acquire compelling evidence against these criminals. These examples illustrate the crucial role that electronic surveillance can play in these cases:

- In a 1998 investigation of 19 members and associates of the Genovese and Bonanno organized crime families, electronic surveillance was the essential component that enabled law enforcement to crack a sophisticated stock market manipulation scheme in which these families took control of several corporations and brokerage firms through bribery and intimidation.
- In "Project Onig," the FBI, working with Italian and Colombian law enforcement, targeted a massive drug trafficking network involving Italian organized crime groups

and Colombian cartels. The investigation, which relied extensively on electronic surveillance conducted in the United States, Italy, and Colombia, culminated in 1994 with the arrest and indictment of 33 individuals in the United States and 74 others in Italy.

17. The 1997 Federal Wiretap Report issued by the Administrative Office of the United States Courts indicates that the clear majority of all Title III interception orders authorized by state and federal courts in 1997 were devoted, at least in part, to fighting the critical national problem of drug trafficking. The fundamental harm to society caused by the illegal drug trade is incalculable. Drug trafficking activity inflicts multiple harms upon our society through kidnapings, murders, drive-by shootings in neighborhood streets, thefts and robberies committed by drug dealers and desperate drug addicts, violent turf battles over control of drug distribution in particular areas, lost productivity of drug addicts, health care expenses related to treatment and to drug-related casualties, and the sad phenomenon of a generation of drug-dependent babies. Most of the drugs that are largely responsible for these problems are those (such as cocaine and heroin) that must be imported into the United States, generally by highly-organized criminal groups, drug trafficking cartels, and other syndicates, and thereafter transported across vast distances and distributed widely within the United States. Even drugs which can be produced locally, such as methamphetamine, are often distributed through extensive networks. The cartels and other organizations responsible for this illegal enterprise rely heavily on telecommunications to coordinate their efforts.

- In 1996, after several failed attempts to infiltrate the interstate drug trafficking

activities of a Los Angeles-based street gang, law enforcement initiated two court-authorized wiretaps over telephones used in conjunction with drug purchases made by an informant. Within the first month of monitoring, agents were able to identify the telephones and a pager used by a principal member of the organization and to obtain court orders to intercept communications over these facilities. Information learned from the communications intercepted enabled the FBI to identify many of the customers, suppliers, facilitators, and interstate distributors linked to the drug trafficking organization, as well as to identify numerous individuals involved in laundering the drug proceeds. As more pieces of the organization were identified, law enforcement was able to utilize this information to initiate spin-off wiretaps on numerous suppliers and distributors across the country, as well as other targets linked to the organization. Over the course of 10 months, 19 court orders were obtained to conduct wiretaps on 18 telephone lines, 9 cloned cellular telephones and 9 pagers. This in turn led to numerous drug interdictions across the country, resulting in the seizure of more than 31 kilograms of cocaine, more than 6 kilograms of heroin, 25 pounds of marijuana, one kilogram of methamphetamine, one-half ton of methamphetamine precursor, more than $400,000 in U.S. currency, and the forfeiture of two residential properties and more than 20 vehicles. At the culmination of the investigation, 82 subjects were charged nationwide with violations of federal drug, money laundering, firearms and conspiracy laws. As of January 1999, 70 of these defendants have been convicted. The Los Angeles case, while significant, is not atypical.

- In another major drug investigation on the Southwest border, more than 30 Title III orders (involving telephone, pager and listening devices) were employed over an 18 month period. Information learned as a result of the interceptions led to the seizure of more than 2 tons of cocaine and 45,000 pounds of marijuana in the United States and Mexico. Of the more than 20 individuals arrested and indicted, several of the principals have been charged with conducting a continuing criminal enterprise, which carries a mandatory 20 year term of imprisonment. The hierarchical structure of the organization, the identity of the principals and their role in supervising the drug trafficking activity necessary to obtain these convictions could not have been established without the information acquired through the Title III interceptions. Information obtained through electronic surveillance in this case also resulted in a number of spin-off investigations involving bribery and corruption.

18. In addition to providing law enforcement with the information needed to identify the organization's operatives and to trace the illegal drug proceeds, electronic surveillance often provides the only reliable method of linking the drug organizations' leaders with the enterprises. Because national and international drug chieftains and local drug “kingpins” do not generally participate directly in drug buys or shipments, electronic surveillance frequently provides the only direct and persuasive evidence that will support a criminal conviction of these drug "kingpins." Consequently, information derived from electronic surveillance is essential in successfully prosecuting those at the highest level of the drug trade. For example, one notorious Los Angeles crime figure, who had been the subject of numerous multi-agency investigations for a decade, consistently avoided

prosecution by insulating himself within his organization and murdering those associates he believed were cooperating with law enforcement. Finally, in 1996, a confidential informant was able to engage the subject in multiple heroin transactions. These transactions led to a series of Title III surveillance orders, which allowed agents to identify how this individual structured his drug organization and managed its operatives, including the suppliers, interstate distributors, facilitators and the launderers of the drug proceeds. When they intercepted a conversation describing the details of the target's involvement in a murder-for-hire scheme while monitoring a Title III interception, the agents terminated the electronic surveillance and arrested the target. Without the use of electronic surveillance in this case, agents would not have been able to develop the crucial evidence needed to indict and successfully prosecute this notorious criminal and 15 other people involved in his criminal organization.

19. Corruption and fraud undermine the public's respect for and confidence in governmental institutions and the rule of law. By their nature, corruption and fraud flourish in secrecy, hidden from public view. As a result, normal overt investigative techniques are often unavailing in the investigation of these crimes. Hence, law enforcement has often found that electronic surveillance and undercover operations are essential to effectively detect, investigate, and prosecute these crimes. Electronic surveillance has also played an indispensable role in countering governmental fraud. For example, the "Operation Illwind" investigation (which was largely based upon 18 months of Title III interceptions) had a tremendous impact upon fraud and abuse both within the government, and within industries that contract with the government. Similarly, electronic surveillance utilized extensively in

“Operation Gold Pill” assisted in the successful prosecution of numerous persons responsible for extensive health care violations that posed a significant threat to public safety.

20. As a general matter, society's most dangerous criminals and criminal organizations are also the ones most likely to take advantage of technologically advanced telecommunications and services. Law enforcement has observed that criminal organizations are increasingly looking for new ways to avoid surveillance by manipulating new technologies — for example, by frequently changing their telecommunications devices and telephone numbers, modifying and reprogramming their cellular telephone identification numbers and codes, and utilizing call-forwarding and other network features. This increasing use of new technologies has eroded law enforcement's ability to protect the public and effectively enforce the law.

21. Full implementation of CALEA is essential to the maintenance of electronic surveillance as an effective law enforcement tool, and to the prevention of the multitude of public harms that would result from the loss or diminution of its effectiveness. All of the "punch list" items that the government has asked the Federal Communications Commission to incorporate into its rule to ensure full compliance with the Act are important to law enforcement’s continued ability to make effective use of electronic surveillance.

A. Conference Call Content

The ability to intercept the pertinent communications of all parties in a conference call supported by a subscriber's service or facilities is important because, for example, co-conspirators conversing while placed on hold during a conference call may make statements that incriminate them or other conspirators, or that could,

if intercepted, enable law enforcement to act in time to prevent loss of life. We have found that conference calls are frequently used by participants in crime, and particularly by prison inmates. Moreover, it is common for a third party to set up a conference call for criminal participants without actually participating in the conversation once the conference has begun.

B. Party Join/Hold/Drop Information

The inability to know when parties are added to, dropped from, or placed on hold during conference calls could have serious legal and evidentiary consequences for law enforcement. Without messages indicating these events, law enforcement will find it difficult to determine who is participating in a call at specific moments. This information is important, because demonstrating a potential conspirator's guilt may require showing that the conspirator heard particular statements made in the course of a conference call, or that he made statements that another conspirator heard. Conversely, this information may establish that a person is innocent because he was not on the conference call when particular criminal conversations occurred. It is therefore important that this information be provided to law enforcement.

C. Subject-Initiated Dialing and Signaling Information

Subject-initiated dialing and signaling activity, indicating the subject's use of such features as call forwarding, three-way calling and call transfer, must be collected by law enforcement in order for law enforcement to be able to know who was participating in a call at various points — information which law enforcement must have in order to make effective use of electronic surveillance.

D. In-Band and Out-of-Band Network Signaling

Information relating to network-generated signaling is often of significant investigative importance. For example, the fact that a particular call attempt resulted in ringing, as opposed to a busy signal, may require a different interpretation of the subsequent actions of the subject who made the call attempt. Law enforcement has encountered cases in which criminals used ringing signals as a way of conveying pre-arranged messages to each other without having to engage in direct conversations over the telephone.

The message waiting notification is another form of signaling which is increasing in investigative importance. A network-generated message waiting notification alerts the subject that he received a call and that the resulting communication is waiting in the subscriber's voice mail box. A person may elect to retrieve his messages by remotely accessing the voice mail box directly, that is, by using a phone other than the subscriber's telephone. Without notification that a voice mail message is waiting, law enforcement may have no idea that a call was made that resulted in a communication left in the subscriber's voice mail box.

Law enforcement in Portland, Oregon recently experienced such a problem in the course of an organized crime drug investigation, when the target purchased numerous cellular telephones apparently for the sole purpose of directing incoming calls to the voice mail boxes assigned to each phone. Instead of using his cell phone to retrieve the messages, however, he would use different public telephones in an effort to avoid electronic surveillance. Using this method, the subject obtained, solely

through use of his voice mail, all of the communications necessary to conduct his drug transactions. Despite the best efforts of law enforcement and the local cellular service provider, it was not possible to replicate the subject's messages.

E. Timing Requirements

Law enforcement needs solid evidence to convict criminals. Furthermore, law enforcement often needs electronic surveillance quickly, in order to be able to act in time to prevent crimes. This means that information identifying the origin, direction, destination, or termination of a call must be provided to law enforcement both quickly and in a manner that allows it to be associated — with considerable accuracy — with the communications included in the call. If this information is delivered hours or days after the communication, law enforcement may be unable to act in time to prevent planned crimes that it has heard discussed in the communication. And if the information is not delivered in a manner that can be accurately correlated with particular communications, law enforcement may be unable to make effective use of electronic surveillance information in a trial, when the defendant challenges law enforcement's assertions regarding the timing and sequence of events that occurred in the course of an intercepted communication.

Such delays were experienced with a Title III order on a cellular phone utilized by the leader of a Gangster Disciples "gang set" to direct the gang's drug trafficking and other criminal activities. From the inception of the order, law enforcement was not receiving the dialed digits associated with the incoming calls. Despite a subsequent court order compelling the carrier to provide records of the call data on

a daily basis, law enforcement still did not receive the necessary information in a timely manner. Consequently, law enforcement was unable to precisely correlate the incoming call identifying information with the associated call content.

F. Surveillance Integrity

Our need for solid evidence, and our legal obligation to protect the privacy of communications not authorized to be intercepted, also means that we must be able to monitor the integrity of our electronic surveillance. The integrity of a surveillance effort may be affected by changes in a subscriber's features or services, such as the addition of call forwarding, call waiting, conference calling, or the disconnection or suspension of service. In order to be able to use the information developed through electronic surveillance as evidence in a prosecution and to protect, to the greatest extent possible, the privacy of communications that are not covered by a surveillance order, we must have the ability to verify that an interception is collecting all of the information that is covered by a Title III order and is not connected to the wrong subscriber.

Law enforcement repeatedly encounters criminals who frequently change their phones and/or their phone numbers. This is a particular problem with criminals who use cellular telephones, especially prepaid cellular telephones. Law enforcement needs to be able to ensure that court ordered electronic surveillance in such cases can capture all communications covered by a surveillance order. To this end, law enforcement must be quickly notified of changes in the target's phone or phone number.

In one drug investigation, the subject changed the phone number of his cellular phone about once a week. Whenever the phone number of that facility changed, the pen register authorized to receive dialing information from that facility stopped recording information. Law enforcement was required to contact the cellular service provider whenever it noticed that the pen register was no longer receiving data, and request that the subject's service again be routed to the pen register. The cellular provider explained that it could not "flag" the subject's account to alert its personnel to notify law enforcement of changes, because it could not guarantee that the subject would not be inadvertently notified of the flag on his account. A requirement that changes in feature status be provided on an automated basis would eliminate these concerns.

G. Post Cut-Through Dialing

In order to preserve its ability to learn the identity of persons whom a target is calling, law enforcement must be given access to all of the dialed digits that identify a call destination, including those dialed after "cut-through"— for example, the number of a call destination dialed after accessing a long-distance service such as "1-800-SPRINT." Indeed, if law enforcement does not have access to digits that are dialed after "cut-through," criminals will most certainly use these services specifically to evade surveillance.

H. Delivery Interface

Finally, without some reasonable limit on the number of different interface protocols used in providing electronic surveillance information to law enforcement,

collecting all of the information it is legally authorized to receive will prove extremely expensive and difficult. Imposing such a limit will ensure that law enforcement is, as a practical matter, able to collect all of the information it is legally authorized to collect.

22. In summary, electronic surveillance is a critical tool for law enforcement at all levels of government working to prevent and punish the most serious criminal threats facing our society. Congress enacted CALEA because it understood that any serious threat to law enforcement's ability to use this tool pursuant to court orders would therefore be a severe threat to society itself. Should law enforcement lose the ability to conduct effective electronic surveillance, the result would be:

— the loss of life and substantial economic harm, attributable to law enforcement's weakened ability to prevent and deter terrorist acts and murders,

— an increase in unprosecuted kidnapings, and in the amount of time kidnap victims are held before law enforcement can intervene,

— the growth of organized crime groups and gang activity, and the resulting increase in illegal drug and weapons trafficking, corruption of legitimate business, industry, labor unions and public officials, and economic harm to business and society,

— an increase in unprosecuted criminal cases of all kinds, and the potential for an increase in acquittals and hung juries resulting from a lack of direct and persuasive electronic surveillance evidence.

While this list is by no means exhaustive, I can say with certainty that full

implementation of CALEA is essential to our efforts to combat these threats. I urge the Commission to fully implement Congress' purpose in enacting CALEA by including all of the "punch list" items in its rule, thereby guaranteeing that carriers will provide law enforcement with all of the capabilities required by law to effectively carry out court-authorized electronic surveillance.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge. Executed on January 27, 1999.

Respectfully submitted,

Louis J. Freeh
Director,
Federal Bureau of Investigation
United States Department of Justice
Washington, D.C. 20535