CRM / WIRETAPPING

ROUTING AND TRANSMITTAL SLIP	DATE	September 13, 1996
TO: (Name, office symbol, room number, Agency/Post)	Initials	Date
1. Merrick Garland		
2. Cathy Russell		
3. Casey Cooper		
4.		
5.		

REMARKS:

Attached is a draft of the wiretap-touting report that the DAG asked me to prepare. Please let me know what you think of it.

DO NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions.

FROM: (Name, org. symbol, Agency/Post)	Room No. --Bldg.
	4116 - MAIN
JONATHAN D. SCHWARTZ Counsel to the Deputy Attorney General	Phone No. 514-4375

SOLVING MAJOR CRIMES THROUGH WIRETAPPING: THE UNTOLD STORY

1. BACKGROUND

Communications networks bring law-abiding citizens together and facilitate economic growth, productivity, and prosperity. But they also connect dangerous and violent criminals and terrorists, facilitating their criminal activities. Like legitimate business organizations, criminal and terrorist organizations rely heavily upon telephones, pagers, computers, and other communications networks to plan and bring about their objectives. Congress recognized this when it enacted the first comprehensive electronic surveillance legislation in Title III of the Omnibus Crime Control and Safe Streets Act of 1968. At that time, Congress was cognizant of the great harm and threat to society posed by organized crime families and groups, and the great investigative and prosecutive importance that wiretapping held in properly dealing with that threat. Nearly thirty years later, criminal organizations of all stripes, and increasingly terrorist organizations, continue to pose the greatest threats to the public safety in our country. As demonstrated in the next section, law enforcement has had great success in meeting the challenges posed by these organizations because of its ability to conduct electronic surveillance of their activities.

Congress has recognized that electronic surveillance, in terms of its very nature of surreptitious interceptions of private communications, could pose an extremely serious threat to personal privacy. Thus, Congress was careful to balance in the Title III legislation the competing considerations of law enforcement's legitimate needs and individuals' recognized privacy rights. There are numerous constraining provisions in Title III, many of which are based on, or expand, constitutionally-based protections, which ensure that electronic surveillance is used judiciously by law enforcement and with abundant deference to the privacy of individuals' communications. For example, high-level Department of Justice approval is required before an electronic surveillance application may be submitted to a federal district court judge, who must carefully monitor the progress of the electronic surveillance if he or she approves the application; an application must show that normal investigative techniques have been tried or considered and will not work, or are too dangerous; the electronic surveillance must be related to specific federal felony offenses; notice must be provided to those who are the subjects of the electronic surveillance, subsequent to the conclusion of the interception period; and unlawful interceptions are punishable by criminal fines or imprisonment. Further, electronic surveillance may not be employed against individuals who are solely exercising their First Amendment rights. The restrictions contained in Title III

also restrict the government's ability to intercept privileged communications, such as those between an individual and his lawyer.

An analysis of the number of electronic surveillance authorizations granted over the years demonstrates that such authorizations have been obtained at reasonable levels, reflecting the fact that electronic surveillance has been used judiciously. (See Appendix A). Federal law enforcement uses electronic surveillance principally in investigations of the largest or most aggravated criminal or terrorist organizations, such as the drug-trafficking cartels and major drug organizations. The Wiretap Report -- the annual Department of Justice report on the use of electronic surveillance, which includes state statistics along with the federal numbers -- states that narcotics investigations were the subject of approximately 69 percent of all Title III electronic surveillance efforts conducted in 1995. The next five highest categories of violations targeted for the use of electronic surveillance in 1995 pertain to racketeering; gambling; other or unspecified felonies; homicide and assault; and extortion, including usury and loansharking.

Although it is difficult to obtain completely up-to-date numbers as to all federal agencies' ongoing and outstanding investigations at any one point in time, it would be a fairly conservative figure, when considering all federal agencies that conduct criminal investigations, to estimate a total of 100,000 federal investigations at any one time. This figure is then contrasted with the 1,128 federal Title III electronic surveillance authorizations granted in Calendar Year 1995, resulting in an estimate of one percent for the figure of federal investigations in which Title III electronic surveillance was utilized. This number alone shows great restraint in the use of this valuable investigative technique.

It should be borne in mind that there are substantial fiscal restraints imposed upon law enforcement agencies that seek to conduct electronic surveillance. The implementation and execution of electronic surveillance court orders is very resource intensive, since, among other things, wiretaps require around-the-clock monitoring and, in many cases, the use of expensive translators. As reported in the 1995 Wiretap Report, the cost associated with an average federal law enforcement electronic surveillance wiretap was $72,390. Obviously, given such an expense, use of this technique by law enforcement is necessarily selective; it is typically reserved for use only against those criminal or terrorist organizations of greatest investigative concern.

Federal law enforcement's adherence to the statutory requirements set forth in Title III is demonstrated, in part, by

the relatively few number of cases where the admission at trial of, or use of, electronic surveillance-based evidence has been successfully contested, even when considering figures that combine these numbers for federal and state matters. In this regard, it is worth noting that the Department of Justice is unaware of any congressional complaints or concerns in terms of the electronic surveillance laws having been overused or substantively abused by federal law enforcement authorities.

2. THE UNTOLD STORY

As noted above, wiretapping has been a tool of the utmost importance in many types of criminal investigations, especially those involving serious and violent crime, organized crime, drug trafficking, corruption, and fraud. Beyond this, however, electronic surveillance has been uniquely valuable, indeed of critical importance, in protecting the public and in saving innocent lives. There have been numerous cases where law enforcement agencies, by using electronic surveillance, have not only solved particularly serious crimes (with prosecutors successfully prosecuting those responsible for them), but they have also been able to prevent the perpetration of life-threatening crimes. This unique capability frequently permits law enforcement, having intercepted the communications of criminals or terrorists who are conspiring to murder individuals and/or groups of individuals, to respond promptly to these planned attacks and often to prevent the execution of their violent plans.

The following case summaries are just a sample of the major law enforcement investigations where electronic surveillance was critical to a successful resolution of the matter, whether obtaining the conviction of drug traffickers and the forfeiture of million of dollars in drug assets, or in preventing the destruction of government property and the loss of innocent lives. Generally, what distinguishes these investigations is the extremely secretive and sophisticated nature of the targeted individuals, whose knowledge of law enforcement techniques, along with their intense fear of being detected and arrested, leads them to be highly cautious in their dealings with persons who are not well known to them. These efforts combine to make traditional investigative methods much less likely to be successful. These cases also involve very complex offenses and/or a large number of defendants. It is fair to say that in each of the Title III cases, the wiretaps and bugs were <u>absolutely essential</u> to the arrests and prosecutions of the defendants, along with the seizure of millions of dollars in forfeitable assets from the defendants.

The Commission Case - Organized Crime

In September 1983, the Federal Bureau of Investigation (FBI) began the first in a series of court-authorized wiretaps and bugs targeting "the Commission" - the bosses of organized crime's five leading families. The Title III electronic surveillance in this investigation was employed continuously for 18 months and was extremely productive, providing the FBI with the details of organized crime-related activities that were well beyond the knowledge of any FBI informant. The information obtained from the Title III surveillance was used to put together an airtight case against the defendants. Based in large part on the electronic surveillance information, the defendants were charged in the Southern District of New York with racketeering activities that included murders, loansharking, labor pay-offs, and extortion in the concrete industry in New York. Eight defendants were convicted, including the heads of the Genovese, Lucchese, and Colombo organized crime families.

Paul Castellano/John Gotti - Organized Crime

In the early 1980s, the FBI commenced a Title III investigation of Paul Castellano, the reputed boss of the Gambino organized crime family. Agents installed court-authorized bugs in Castellano's residence. Conversations intercepted over those bugs revealed that Castellano's organization was involved in numerous racketeering activities, including international car theft and conspiracy to murder. In February 1986, six of Castellano's associates were convicted of running the car theft ring.

In December 1985, Castellano was murdered by associates of John Gotti in a power struggle for control of the Gambino family. FBI agents installed court-authorized bugs and wiretaps in a social club frequented by Gotti to obtain evidence of the murder. Based upon intercepted conversations, Gotti was convicted in the Eastern District of New York in April 1992 of racketeering and conspiring to murder Castellano. Gotti is currently serving a sentence of multiple terms of life imprisonment without the possibility of parole.

Patriarca Family - Organized Crime

In 1989, FBI agents placed a court-authorized bug inside a residence outside Boston, Massachusetts, and successfully recorded an induction ceremony involving the Patriarca organized crime family. Based on evidence obtained from the bug in the residence, and from bugs placed in various automobiles used by Patriarca associates, eight Patriarca associates were convicted of racketeering in the District of Massachusetts in August 1991,

and Patriarca pleaded guilty to racketeering in November 1991. As a result of this successful prosecution, the leadership of this crime family was severely debilitated. Other court-authorized interceptions utilized during this investigation resulted in the overhearing of conversations in which Patriarca associates discussed six previous murders and planned the murder of three other persons. The FBI successfully prevented two of the planned murders.

Stanfa Racketeering Case - Organized Crime

In September 1991, the FBI began conducting court-authorized electronic surveillance at a location used as a meeting place by members of Philadelphia organized crime. The investigation targeted the boss, underboss, consigliere, and other members and associates who met regularly at the location, and continued for approximately two years. It was extremely productive, leading to solid evidence of murder, extortion, and other serious racketeering offenses, resulting in the conviction of Philadelphia organized crime boss John Stanfa and his key associates.

The Pizza Connection - Organized Crime

In March 1984, after an investigation that included over one year of continuous court-approved Title III wiretaps, the United States Attorney for the Southern District of New York charged 31 persons with running a huge international narcotics and money-laundering ring that, for over five years, had smuggled heroin worth approximately $1.65 billion into the United States. The heroin was distributed through organized crime-controlled pizza parlors in small towns. The operation was headed by Gaetano Badalamenti, one of the world's leading heroin importers, and Salvatore Catalano, underboss of the Carmine Galante crime family. After a 17-month trial in which hours of wiretapped conversations were played to the jury, 17 defendants were convicted, and only one was acquitted of all charges.

Daniel Depew/Dean Lambey - Child Pornography

In August 1989, Daniel Depew and Dean Lambey were arrested by the FBI and subsequently charged with conspiracy to kidnap a male child whom they planned to molest and then kill for a pornographic "snuff" film. The investigation had begun six months earlier when an undercover police officer tapped into a computer bulletin board system used by child pornographers. Lambey provided the undercover officer with his telephone number as a contact point. A court order was then obtained authorizing the FBI to tap Lambey's telephone, and the FBI intercepted

conversations involving Lambey's and Depew's kidnapping plans, including their plan to dispose of the victim's body by washing down the corpse with muriatic acid. Both men were convicted of kidnapping and related charges in federal court in the Eastern District of Virginia, and both received lengthy prison terms.

Joseph Meling - Murder by Product Tampering

In February 1991, three Seattle-area residents ingested capsules of Sudafed (an over-the-counter cold remedy) that had been laced with cyanide, resulting in the deaths of two of the three, and serious injury to the third, Jennifer Meling. In March 1991, FBI agents targeted Jennifer's husband, Joseph Meling, as the prime suspect in the product tampering. While the initial investigation failed to provide the necessary evidence of Meling's involvement, it did provide probable cause to support the court-authorized interception of communications occurring involving Meling's parent's residence, where he was residing after his wife initiated divorce proceedings against him. Near the end of the interception period, agents overheard a discussion in the residence related to the source of the cyanide. This conversation provided agents with leads that led to Meling's arrest, indictment, and conviction.

Herrera-Buitraga Organization - Cali Cartel

One of the most successful use of wiretaps in a narcotics investigation occurred in connection with a Drug Enforcement Administration (DEA) investigation of the Herrera-Buitraga organization in the Eastern District of New York. The investigation, which targeted New York City-based operatives for the Cali, Colombia, cocaine cartel, was largely dependent upon approximately 18 months of continuous court-authorized wiretaps of communications occurring over cellular telephones used by members of the various New York cells reporting to major drug lords in Cali. The Title III-intercepted conversations led directly to millions of dollars worth of cocaine and cash, which the DEA seized at various points in the investigation. At the conclusion of the taps in December 1991, the DEA arrested more than 100 individuals and seized $14.6 million in cash.

Operation Illwind - Defense Procurement Fraud

Between January 1987 and July 1988, the FBI conducted a series of court-authorized interceptions of the communications of several defense procurement consultants in the District of Columbia, the Eastern District of Virginia, the Middle District of Florida, and the Eastern District of New York. The investigation, known as "Operation Illwind," focused upon

allegations of bribery and fraud being committed by Department of Defense employees, contractors, and consultants in the award of massive procurement contracts for the military. As a result of information gleaned from the 18 months of interceptions, the FBI executed approximately 45 search warrants and seized massive amounts of personal and corporate records. The investigation resulted in 64 convictions and $622 million in fines, including a $190 million fine assessed against the Unisys Corporation.

Operation Polar Cap - Money Laundering

In November 1991, after 18 months of continuous court-authorized wiretaps and bugs in several jurisdictions in the United States, the Customs Service broke up the largest international money laundering organization ever prosecuted in this country. Code-named "Operation Polar Cap," this investigation determined that the organization used precious-metals companies as fronts, funneling hundreds of millions of dollars through United States banks to Colombian cocaine cartels. At its peak, this group was laundering $60 million in drug proceeds a month. Law enforcement agents used the wiretaps to tie together evidence from informants and an active undercover operation. The key wiretaps provided the critical link between Stephen Saccoccia, the head of the money laundering operation in the United States, and Duvan Arboleda, the Miami-based conduit for the Colombian drug cartels, and a close associate of Medellin drug lord Pablo Escobar. In the end, fifty-six individuals were arrested and more than $10.7 million seized.

Walter Moody - Murder of a Federal Judge

In December 1989, Robert Vance, a judge on the United States Court of Appeals for the Eleventh Circuit, was killed by a bomb mailed to his residence in Georgia. In April 1990, federal agents targeted Walter Moody as a suspect in the bombing, and, pursuant to a court order, placed bugs in Moody's residence. Agents learned from the bugs that Moody talked to himself about the bombing. In June 1990, Moody was arrested on an unrelated charge, and agents placed a bug in Moody's prison cell. In June 1991, Walter Moody was convicted in the Northern District of Georgia of first degree murder in the killing of Judge Vance. Prosecutors used evidence obtained from the bug in the prison cell to prove that Moody created and sent the bomb.

Chinese Organized Crime - Gang Kidnapping

On March 18, 1994, four Chinese nationals were kidnapped by six men from a location in New York City. This case, like others recently, concerned illegal alien smuggling. Over the following

day and a half, 15-20 telephone calls were made by the kidnappers to an associate of the victims demanding money in exchange for the safe release of the victims. The kidnappers provided the associate of the victims with the number of a cellular phone and instructed the associate to contact them on that telephone. On March 19, 1994, the Attorney General authorized the emergency interception of communications over the cellular telephone used by the kidnappers. The wiretap was credited with leading to a successful resolution of the situation: the four victims were recovered, relatively unharmed, and 12 arrests were made.

D.C. Police Probe - Public Corruption

In 1994 and 1995, FBI agents conducted an extensive investigation into suspected corruption in the Metropolitan Police Department of the District of Columbia. An integral part of that investigation involved court-authorized electronic surveillance of the main targets, who were providing protection for criminal activities of undercover agents posing as major drug distributors. The investigation led agents to identify a dozen corrupt police officers operating within the ranks of the Metropolitan Police Department. The corrupt officers were arrested, and nine have since pleaded guilty to various federal charges and been given lengthy prison sentences.

Operation Horse Collar - Drug Trafficking and Gang Violence

The extensive use of electronic surveillance was critical to the successful conclusion of a lengthy FBI-led task force case targeting drug trafficking and gang activities in New York City during the late 1980s and early 1990s. During this investigation, code-named "Horse Collar," numerous court-authorized interceptions were conducted, and the information obtained was critical in achieving 167 convictions and the seizure of over $8 million in assets and substantial quantities of drugs. Evidence also was obtained leading to the resolution of 40 New York-area homicides, including the murders of a New York City police officer and a New York State parole officer. The FBI also reported that, following this investigation, there was a substantial drop in drug-related homicides in the area.

Rukbom - Domestic Terrorism

In Rukbom, a domestic terrorism case, the El Rukn street gang in Chicago, attempting to act as a surrogate for the Libyan Government, proposed to shoot down a commercial airliner with a stolen military rocket in return for financial remuneration. Court-authorized electronic surveillance enabled law enforcement to step in and prevent this attack, thereby saving over one

hundred lives (and possibly many more) by averting a domestic disaster similar to the terrorist bombing of Pan Am Flight 103 over Scotland.

Zorro II - Cali Cartel's Operations in the United States

An extremely successful use of wiretaps in a narcotics investigation occurred in DEA's investigation of the Cali Cartel and its operations in the United States. This investigation, code-named "Zorro II," was concluded in the spring of 1996 and utilized numerous court-authorized wiretaps that were conducted over nine months in nine judicial districts. Based upon information produced by the wiretaps, over 130 persons were arrested, and 5,598 kilograms of cocaine and approximately $9 million in cash drug proceeds were seized.

Operation Gold Pill - Health Fraud

Between 1989 and 1992, Title III electronic surveillance was used successfully in a major health-fraud investigation, code-named "Operation Goldpill," which was conducted by the FBI in several districts throughout the United States. The investigation centered on the illegal diversion of prescription drugs from legitimate pharmacies to the black market, where the drug were resold without proper labels or other safety information to illegitimate pharmacies, which, in turn, resold the drugs to unwitting consumers. In total, 156 persons were convicted nationwide of fraud and related charges, and $19 million was imposed as fines or court-ordered restitution, or received in recoveries.

3. CONCLUSION

Federal law enforcement's use of electronic surveillance has been consistent with the spirit of, and the strict statutory procedures set forth in, the electronic surveillance laws. As demonstrated above, the investigative and prosecutive benefits of court-authorized electronic surveillance are clear. It has provided sufficient means to enable federal law enforcement to carry out its principal mission -- protecting the public safety and solving crimes committed by major criminal organizations.