CELLULAR TELEPHONE FRAUD

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTH CONGRESS

FIRST SESSION

ON

CELLULAR TELEPHONE FRAUD

SEPTEMBER 11, 1997

Serial No. 77

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

55-946 WASHINGTON : 1997

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-058343-8

COMMITTEE ON THE JUDICIARY

HENRY J. HYDE, Illinois, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
BILL McCOLLUM, Florida
GEORGE W. GEKAS, Pennsylvania
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
STEVEN SCHIFF, New Mexico
ELTON GALLEGLY, California
CHARLES T. CANADY, Florida
BOB INGLIS, South Carolina
BOB GOODLATTE, Virginia
STEPHEN E. BUYER, Indiana
SONNY BONO, California
ED BRYANT, Tennessee
STEVE CHABOT, Ohio
BOB BARR, Georgia
WILLIAM L. JENKINS, Tennessee
ASA HUTCHINSON, Arkansas
EDWARD A. PEASE, Indiana
CHRISTOPHER B. CANNON, Utah

JOHN CONYERS, JR., Michigan
BARNEY FRANK, Massachusetts
CHARLES E. SCHUMER, New York
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
STEVEN R. ROTHMAN, New Jersey

THOMAS E. MOONEY, *Chief of Staff-General Counsel*
JULIAN EPSTEIN, *Minority Staff Director*

SUBCOMMITTEE ON CRIME

BILL McCOLLUM, Florida, *Chairman*

STEVEN SCHIFF, New Mexico
STEPHEN E. BUYER, Indiana
STEVE CHABOT, Ohio
BOB BARR, Georgia
ASA HUTCHINSON, Arkansas
GEORGE W. GEKAS, Pennsylvania
HOWARD COBLE, North Carolina

CHARLES E. SCHUMER, New York
SHEILA JACKSON LEE, Texas
MARTIN T. MEEHAN, Massachusetts
ROBERT WEXLER, Florida
STEVEN R. ROTHMAN, New Jersey

PAUL J. MCNULTY, *Chief Counsel*
GLENN R. SCHMITT, *Counsel*
DANIEL J. BRYANT, *Counsel*
NICOLE R. NASON, *Counsel*
DAVID YASSKY, *Minority Counsel*

CONTENTS

HEARING DATE

OPENING STATEMENT

WITNESSES

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

CELLULAR TELEPHONE FRAUD

THURSDAY, SEPTEMBER 11, 1997

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to call, at 9:24 a.m. in Room 2141, Rayburn House Office Building, Hon. Bill McCollum (Chairman of the Subcommittee) presiding.

Present: Representatives Bill McCollum, Steven Schiff, Steven E. Buyer, Steve Chabot, Bob Barr, Asa Hutchinson, George W. Gekas, Howard Coble, Sheila Jackson-Lee, Martin T. Meehan, Robert Wexler, Steven R. Rothman.

Also present: Paul J. McNulty, chief counsel; Glenn R. Schmitt, counsel; Kara Norris, staff assistant; David Yassky, minority counsel.

OPENING STATEMENT OF CHAIRMAN MCCOLLUM

Mr. MCCOLLUM. Please come to order. Today, we consider an issue which this Subcommittee has never before considered—cellular telephone fraud. Anyone who has experienced having their cellular telephone "cloned" will testify that this problem is, at the very least, a major inconvenience. But in reality, this activity is much more than an inconvenience. It is also a major crime problem.

Each year, the cellular telephone industry loses millions of dollars in revenue because of the criminal actions of persons who are able to reconfigure cellular telephones so that their calls from such phones are billed to other phones owned by innocent third persons. Often these cloned phones are used to place hundreds of calls, often long distance, even to foreign countries, resulting in thousands of dollars in air time and long distance charges. Cellular telephone companies do not require their customers to pay for any charges illegally made to their account, no matter how great the cost. But we must all remember that some portion of the cost of these illegal telephone calls is passed along to cellular telephone consumers as a whole.

And as important as fraud on these companies is, there is another, even more serious, aspect to these illegal activities. Many criminals use cloned cellular telephones as a means to facilitate other serious crimes, because their calls are not billed to them, and are therefore much more difficult to trace.

This phenomenon is especially prevalent in drug crimes. Drug dealers need to be in constant contact with their sources of supply

and their confederates on the streets. Traffickers acquire cloned phones at a de minimus cost, make dozens of calls, and then throw the phone away after as little as one days' use.

In the same way, criminals who pose a threat to our national security, such as terrorists, have been known to use cloned phones to thwart law enforcement efforts aimed at tracking their whereabouts.

If cellular telephones were harder to clone, and if the illegal use of these telephones and the devices used to clone them were more likely to be punished, I am confident that this would have an impact in the amount of other crime, especially drug crimes, which take place in this country.

Today, we are going to hear testimony from the law enforcement community concerning this crime. Our first law enforcement witness will be a representative of the United States Secret Service, the law enforcement agency with the lead role in investigating these types of crimes. In addition to their testimony, the Service will demonstrate the relative ease by which a phone can be cloned and used to make illegal telephone calls. We will also hear from the Drug Enforcement Administration and the Federal Bureau of Investigation concerning other crimes in which cloned phones are often used.

And we will hear from a representative of the cellular telephone industry as to the magnitude of the losses it experiences from cellular telephone fraud and the steps it is taking to combat this fraud. Finally, we will hear from a representative of the manufacturers of cellular telecommunications equipment to discuss some of the new innovations that are being made to prevent this type of fraud from occurring.

I am happy to welcome all of the witnesses here today. I believe that your testimony will lead to some productive new legislation.

Mr. MCCOLLUM. I would like to ask if any other Member wishes to make an opening comment. Mr. Gekas.

Mr. GEKAS. Mr. Chairman, I too am grateful for the opportunity to hear the witnesses in this matter, but time constraints will cause me to leave here for a markup in my own committee. But in the meantime, I know that one of the selling features of the testimony will cover the current status of the law and that which we all hope will evolve from these hearings.

As a young prosecutor one time, I remember that the law enforcement establishment in my region conducted a raid on all known gambling purveyors and arrested an individual for having in his possession—in his warehouse—dozens of slot machines. The eventual defense in court was that these were just sitting there and that there was no intent to use them for purposes of gambling. But the statute constituted a slot machine as being gambling, per se; and the mere possession of it, the mere lodging of it, the warehousing of it, just the owning of it and control of it constituted a crime, the lack of intent for which was not going to be a defense.

That is the best corollary that I have in my mind for what we might be attempting to do here. If intent to use a cloning device is going to be an element, then that breeds mischief in the enforcement of law. Looking towards making them criminal, per se, will

probably be the best answer we could conjure up in this circumstance.

So I hope to be able to get the benefit of the testimony even though it might be I would have to read it later. Thank you very much, Mr. Chairman.

Mr. MCCOLLUM. Thank you very much, Mr. Gekas. Mr. Coble, do you have any opening remarks?

Mr. COBLE. Very briefly, Mr. Chairman. Not unlike the gentleman from Pennsylvania, I am going to have to leave to conduct a hearing in our subcommittee as well. Our hearing, Mr. Chairman, involves policy on the Internet. So today it appears that, on the Hill, we are directing attention to people who enjoy stealing in one way or another and that it is not right, it needs to be addressed, and I thank you, Mr. Chairman, for having this hearing today.

Mr. MCCOLLUM. Thank you, Mr. Coble, I appreciate that very much. Since I serve on your Subcommittee, the fact is that we are both focusing on "stealing" as a hearing topic today.

I would like to introduce the first panel at this time. Our first witness is Michael C. Stenger, the Special Agent in Charge of the Financial Crimes Division of the United States Secret Service. He is a 21-year veteran of the Secret Service, having served in Newark, New York City, and Washington, D.C., in both protective and investigative assignments.

In his present position, he heads the division of the Secret Service responsible for the oversight, direction, and coordination of domestic and international criminal investigations involving financial crimes. He received his bachelors degree from Farleigh Dickinson University.

Anthony R. Bocchichio is the Assistant Administrator of the Operational Support Division of the Drug Enforcement Administration. He has served with the DEA and its predecessor agency since 1961. He has served in the New York and Miami field offices and was a Special Agent in Charge of the St. Louis Field Division from 1994 to 1996 when he assumed his present position. He holds a bachelors degree in criminal justice from the State University of New York and a masters degree in public administration from the University of Southern California.

Our third and final witness on this panel is Mr. John Navarrete. He is the Deputy Assistant Director of the Criminal Investigative Division of the Federal Bureau of Investigation. Mr. Navarrete became a Special Agent in 1969 and has served in Miami, Newark, San Juan, and Washington, D.C. In 1994, he became the Special Agent in Charge of the El Paso office. Following that assignment, he was detailed to the Office of National Drug Control Policy as the Assistant Associate Director in charge of federal, state and local drug law enforcement before assuming his present position. He received his bachelors degree from Texas Western College and his masters degree from the University of Texas at El Paso.

Mr. Stenger, if you could open. Your full testimony will be admitted into the record without objection. You may feel free to summarize or present any portion of it that you wish—that will be true for all three of the panel.

Mr. Stenger, please proceed.

STATEMENT OF MICHAEL C. STENGER, SPECIAL AGENT IN CHARGE, FINANCIAL CRIMES DIVISION, UNITED STATES SECRET SERVICE

Mr. STENGER. Thank you, Mr. Chairman and the members of the Committee for letting us have the opportunity today to address you concerning the issue of telecommunication fraud. I would like to point out that with me today is Special Agent Mary Riley of our electronics crime branch who will provide the demonstration and offer to you at a subsequent date our ability to show you some in-depth demonstrations of some of the technical investigative enhancements we use to investigate these activities.

As a law enforcement bureau within the Department of Treasury, the Secret Service is well known for its expertise in the suppression of criminal activity in the area of financial crimes. Along with the investigative expertise gained through interaction with the financial industry comes a clear understanding of the overall infrastructure of the financial system. The telecommunications industry, one of the fastest growing technologies in the world, provides the backbone upon which that industry is built.

In 1994, the addition of telecommunications-specific language to Title 18, United States Code, Section 1029 enhanced the ability of the Secret Service and federal prosecutors in addressing the type of criminal activity associated with telecommunications crimes. A large percentage of the cases brought for prosecution involve the cloning of cellular telephones.

Due to the fact that the statute presently requires the proof of "intent to defraud" to charge the violation, the distributors of the cloning equipment have become elusive targets. These distributes utilize disclaimers in their advertising mechanisms aimed at avoiding a finding of fraudulent intent. This allows for the continued distribution of the equipment permitting all elements of the criminal arena to equip themselves with free, anonymous phone service.

Once a phone is cloned, it is usage can continue until the escalated billing activity is detected by the telephone company or the victim user. This billing activity can translate to extensive fraud losses in a very short period of time. A recent example of this type of activity occurred in West Palm Beach, Florida and Agent Riley will show you exactly how that took place.

Working from the preliminary investigation of the local cellular phone company, our agents arrested a Lebanese national who was conducting a "call sell" operation. A call sell operation typically provides international calling activity for a variety of "customers" through the compromise of telecommunications systems. In this case, the defendant completed calls for customers in the Middle East by utilizing cellular account numbers that had been stolen with a scanner in New York. On a daily basis, the defendant's conspirators would express mail a new list of stolen account numbers to further this 24-hour per day operation. At the time of the arrest, some 26,000 account numbers were seized attributing to losses in the millions of dollars.

Federal, State, and Local investigative agencies have experienced the use of these cloned phones associated with all areas of criminal activity. The ability to obtain anonymous phone service has become an asset to the criminal and an obstacle to law enforcement. In our

experience, the suspects under investigation for the fraudulent use of telecommunications systems are rarely committing this crime exclusively. We have conducted numerous investigations that were initiated as a significant fraud investigation and evolved to coordinated efforts with other agencies to further cases involving narcotics trafficking, weapons dealing and violent crimes in which cloned phones were used.

Also, we have found that the proceeds of this type of crime are used to facilitate other types of criminal behavior and to enhance the criminal life-style.

Our efforts to establish and maintain active working relationships with the telecommunications industry, including the CTIA (Cellular Telecommunications Industry Association), have been extremely productive. The Secret Service supports and encourages a comprehensive effort by the telecommunications industry, the private sector and the law enforcement community to develop and implement security enhancements that will serve to protect everyone from the impact of fraud losses and the use of these mechanisms to further criminal activity.

The Secret Service has been developing and maintaining a dialogue with those interested in the development and protection of the global telecommunications infrastructure. For example, we participate in the National Security Information Exchange (NSIE) which is a subgroup of the National Security Telecommunications Advisory Committee (NSTAC) which includes government and industry representatives that deal with threats, deterrents, vulnerabilities and protection mechanisms that affect the telecommunications infrastructure.

The protection of that system, an integral part of our national infrastructure, will continue as a priority in our investigative initiatives.

Once again, I would like to thank you, Mr. Chairman, and the Committee for their time and their continued support for our efforts in this investigative endeavor. Thank you.

[The prepared statement of Mr. Stenger follows:]

PREPARED STATEMENT OF MICHAEL C. STENGER, SPECIAL AGENT IN CHARGE, FINANCIAL CRIMES DIVISION, U.S. SECRET SERVICE

MR. CHAIRMAN, MEMBERS OF THE SUBCOMMITTEE, THANK YOU FOR THE OPPORTUNITY TO ADDRESS THE SUBCOMMITTEE CONCERNING THE ISSUE OF TELECOMMUNICATIONS FRAUD.

MY NAME IS MICHAEL C. STENGER, AND I AM REPRESENTING THE UNITED STATES SECRET SERVICE IN MY CAPACITY AS THE SPECIAL AGENT IN CHARGE OF THE FINANCIAL CRIMES DIVISION OF THE UNITED STATES SECRET SERVICE.

AS A LAW ENFORCEMENT BUREAU WITHIN THE DEPARTMENT OF TREASURY, THE SECRET SERVICE IS WELL KNOWN FOR ITS EXPERTISE IN THE SUPPRESSION OF CRIMINAL ACTIVITY IN THE AREA OF FINANCIAL CRIMES. ALONG WITH THE INVESTIGATIVE EXPERTISE GAINED THROUGH INTERACTION WITH THE FINANCIAL INDUSTRY COMES A CLEAR UNDERSTANDING OF THE OVERALL INFRASTRUCTURE OF THE FINANCIAL SYSTEM. THE TELECOMMUNICATIONS INDUSTRY, ONE OF THE FASTEST GROWING TECHNOLOGIES IN THE WORLD, PROVIDES THE BACKBONE UPON WHICH THAT INDUSTRY IS BUILT.

UNDERSTANDING THE CRITICAL NEED TO PROTECT THE INTEGRITY OF THE TELECOMMUNICATIONS SYSTEMS, THE SECRET SERVICE HAS MADE IT A PRIORITY TO WORK WITH THE TELECOMMUNICATIONS CARRIERS AND MANUFACTURERS TO IDENTIFY AND ADDRESS VULNERABILITIES IN-

HERENT IN THE DEVELOPMENT OF THEIR SYSTEMS AND CUSTOMER BASE.

THE UNITED STATES SECRET SERVICE HAS AGGRESSIVELY INVESTIGATED FRAUDULENT ACTIVITY ON U.S. TELECOMMUNICATIONS SYSTEMS SINCE THE PASSING OF THE OMNIBUS CRIME CONTROL ACT OF 1984. SINCE 1991, FRAUDULENT ACTIVITY ON WIRELESS TELECOMMUNICATIONS SYSTEMS HAS GROWN EXPONENTIALLY TO A $650 MILLION DOLLAR LOSS ESTIMATED BY THE INDUSTRY LAST YEAR. REFLECTING THAT GROWTH, THE SECRET SERVICE HAS DOUBLED THE NUMBER OF ARRESTS BROUGHT FOR FEDERAL PROSECUTION IN THIS AREA EVERY YEAR SINCE 1991.

IN 1994, THE ADDITION OF TELECOMMUNICATIONS–SPECIFIC LANGUAGE TO TITLE 18, UNITED STATES CODE, SECTION 1029 ENHANCED THE ABILITY OF THE SECRET SERVICE AND FEDERAL PROSECUTORS IN ADDRESSING THE TYPE OF CRIMINAL ACTIVITY ASSOCIATED WITH TELECOMMUNICATIONS CRIMES. A LARGE PERCENTAGE OF THE CASES BROUGHT FOR PROSECUTION INVOLVE THE CLONING OF CELLULAR TELEPHONES. A PROBLEM HAS DEVELOPED REGARDING PERSONS WHO USE, PRODUCE, TRAFFIC IN OR POSSES CLONING EQUIPMENT AND, THEREBY MAKE THE CLONING OF CELLULAR TELEPHONES POSSIBLE. DUE TO THE FACT THAT THE STATUTE PRESENTLY REQUIRES THE PROOF OF "INTENT TO DEFRAUD" TO CHARGE THE VIOLATION, THE DISTRIBUTORS OF THE CLONING EQUIPMENT HAVE BECOME ELUSIVE TARGETS. THESE DISTRIBUTORS UTILIZE DISCLAIMERS IN THEIR ADVERTISING MECHANISMS AIMED AT AVOIDING A FINDING OF FRAUDULENT INTENT. THIS ALLOWS FOR THE CONTINUED DISTRIBUTION OF THE EQUIPMENT PERMITTING ALL ELEMENTS OF THE CRIMINAL ARENA TO EQUIP THEMSELVES WITH FREE, ANONYMOUS PHONE SERVICE.

THE "CLONING" OF A CELLULAR TELEPHONE OCCURS WHEN THE ACCOUNT NUMBER OF A VICTIM TELEPHONE USER IS STOLEN AND REPROGRAMMED INTO ANOTHER CELLULAR TELEPHONE. THE REPROGRAMMING IS ACCOMPLISHED THROUGH THE UTILIZATION OF EQUIPMENT DESIGNED TO DEFEAT THE SECURITY FEATURES IN THE CELLULAR TELEPHONES. THE INDIVIDUAL IDENTITY OF THE CELLULAR TELEPHONE, DESIGNATED THROUGH ITS ELECTRONIC SERIAL NUMBER, SHOULD NEVER BE ALTERED AND THE PHONE ITSELF SHOULD BE MANUFACTURED SO THAT ALTERATION CANNOT OCCUR. MANUFACTURERS ARE DIRECTED THROUGH THE FEDERAL COMMUNICATIONS COMMISSION UNDER SECTION 22.919 REGARDING THE IMPLEMENTATION OF THIS SECURITY FEATURE IN ALL WIRELESS TELEPHONES. THERE IS NO LEGITIMATE USE FOR THE EQUIPMENT SUCH AS THAT DESIGNED TO ALTER THE ELECTRONIC SERIAL NUMBERS IN WIRELESS TELEPHONES. THE MANUFACTURERS OF CELLULAR TELEPHONES ARE CONSTANTLY ENHANCING THEIR DESIGN FEATURES TO THWART THE EFFORTS OF THOSE WHO CREATE EQUIPMENT TO DEFEAT SECURITY FEATURES.

ONCE A PHONE IS CLONED, IT'S USAGE CAN CONTINUE UNTIL THE ESCALATED BILLING ACTIVITY IS DETECTED BY THE TELEPHONE COMPANY OR THE VICTIM USER. THIS BILLING ACTIVITY CAN TRANSLATE TO EXTENSIVE FRAUD LOSSES IN A VERY SHORT PERIOD OF TIME. A RECENT EXAMPLE OF THIS TYPE OF ACTIVITY OCCURRED IN WEST PALM BEACH, FLORIDA. WORKING FROM THE PRELIMINARY INVESTIGATION OF THE LOCAL CELLULAR PHONE COMPANY, OUR AGENTS ARRESTED A FOREIGN NATIONAL WHO WAS CONDUCTING A "CALL SELL" OPERATION. A CALL SELL OPERATION TYPICALLY PROVIDES INTERNATIONAL CALLING ACTIVITY FOR A VARIETY OF "CUSTOMERS" THROUGH THE COMPROMISE OF TELECOMMUNICATIONS SYSTEMS. IN THIS CASE, THE DEFENDANT COMPLETED CALLS FOR CUSTOMERS IN THE MIDDLE EAST BY UTILIZING CELLULAR ACCOUNT NUMBERS THAT HAD BEEN STOLEN WITH A SCANNER IN NEW YORK. ON A DAILY BASIS, THE DEFENDANT'S CONSPIRATORS WOULD EXPRESS MAIL A NEW LIST OF STOLEN ACCOUNT NUMBERS TO FURTHER THIS 24–HOUR PER DAY OPERATION. AT THE TIME OF THE ARREST, SOME 26,000 ACCOUNT NUMBERS WERE SEIZED ATTRIBUTING TO LOSSES IN THE MILLIONS OF DOLLARS.

FEDERAL, STATE, AND LOCAL INVESTIGATIVE AGENCIES HAVE EXPERIENCED THE USE OF THESE CLONED PHONES ASSOCIATED WITH ALL AREAS OF CRIMINAL ACTIVITY. THE ABILITY TO OBTAIN ANONYMOUS PHONE SERVICE HAS BECOME AN ASSET TO THE CRIMINAL AND AN OBSTACLE TO LAW ENFORCEMENT. IN OUR EXPERIENCE, THE SUSPECTS

UNDER INVESTIGATION FOR THE FRAUDULENT USE OF TELECOMMUNICATIONS SYSTEMS ARE RARELY COMMITTING THIS CRIME EXCLUSIVELY. WE HAVE WORKED NUMEROUS INVESTIGATIONS THAT WERE INITIATED AS A SIGNIFICANT FRAUD INVESTIGATION AND EVOLVED TO COORDINATED EFFORTS WITH OTHER AGENCIES TO FURTHER CASES INVOLVING NARCOTICS TRAFFICKING, WEAPONS DEALING AND VIOLENT CRIMES IN WHICH CLONED PHONES WERE USED.

THE PROCEEDS OF THIS TYPE OF CRIME ARE USED TO FACILITATE OTHER TYPES OF CRIMINAL BEHAVIOR AND TO ENHANCE THE CRIMINAL'S LIFESTYLE.

THE TELECOMMUNICATIONS INDUSTRY HAS TAKEN A PROACTIVE APPROACH TO THWART THE EFFORTS OF CRIMINAL ACTIVITY ON THEIR SYSTEMS. THROUGH ENHANCED TECHNOLOGICAL SOLUTIONS TO LAW ENFORCEMENT TRAINING MATERIALS, THE INDUSTRY HAS PROVIDED SOME SOLID SOLUTIONS TO THE GROWING FRAUD PROBLEM. HOWEVER, THE LACK OF UNIFORMITY IN THE IMPLEMENTATION OF THESE FRAUD SYSTEMS MAKES THE SYSTEM AS VULNERABLE AS EVER. THE INCREASE IN THE NUMBER OF FRAUD CASES OPENED BY THE SECRET SERVICE DIRECTLY REFLECTS THE INCREASE IN FRAUD ACTIVITY IN THE SMALLER MARKETS IN THE UNITED STATES. AS THE LARGER MARKETS IMPLEMENT EXPENSIVE TECHNOLOGICAL FRAUD PROTECTION FEATURES, THE INCIDENCE OF FRAUD IN SMALLER CITIES AND COMPANIES HAS INCREASED. SINCE THESE COMPANIES HAVE LESS OF A MARKET SHARE TO DRAW UPON, THE FRAUD LOSSES CAN IMPACT THE COMPANY WITH GREATER SIGNIFICANCE.

FOR EXAMPLE, A SMALL WIRELESS TELECOMMUNICATIONS CARRIER IN THE MIDWEST CONTACTED US REGARDING THE THEFT OF TEN CELLULAR ACCOUNT NUMBERS THAT HAD BEEN USED FRAUDULENTLY IN THE NORTHEAST. THE FRAUD LOSSES ASSOCIATED WITH THOSE ACCOUNTS TOTALED NEARLY $200,000.00. THE VICTIM COMPANY, WHICH EMPLOYED 25 PEOPLE, DID NOT HAVE THE CAPACITY TO ABSORB THOSE LOSSES WITHOUT IMPACTING ON THE WELL–BEING OF THE ENTIRE COMPANY.

OUR EFFORTS TO ESTABLISH AND MAINTAIN ACTIVE WORKING RELATIONSHIPS WITH THE TELECOMMUNICATIONS INDUSTRY, INCLUDING THE CTIA (CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION), HAVE BEEN EXTREMELY PRODUCTIVE. EXPERIENCE HAS SHOWN US THAT THE VULNERABILITIES ARE REAL AND OUR PLANNING AND TIMELY RESPONSE ARE ESSENTIAL IN THE AREAS OF POLICY, TECHNOLOGY AND ENFORCEMENT ISSUES. THE SECRET SERVICE SUPPORTS AND ENCOURAGES A COMPREHENSIVE EFFORT BY THE TELECOMMUNICATIONS INDUSTRY, THE PRIVATE SECTOR AND THE LAW ENFORCEMENT COMMUNITY TO DEVELOP AND IMPLEMENT SECURITY ENHANCEMENTS THAT WILL SERVE TO PROTECT EVERYONE FROM THE IMPACT OF FRAUD LOSSES AND THE USE OF THESE MECHANISMS TO FURTHER CRIMINAL ACTIVITY.

THE SECRET SERVICE HAS BEEN DEVELOPING AND MAINTAINING A DIALOGUE WITH THOSE INTERESTED IN THE DEVELOPMENT AND PROTECTION OF THE GLOBAL TELECOMMUNICATIONS INFRASTRUCTURE. FOR EXAMPLE, WE PARTICIPATE IN THE NATIONAL SECURITY INFORMATION EXCHANGE (NSIE) WHICH IS A SUBGROUP OF THE NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE (NSTAC) WHICH INCLUDES GOVERNMENT AND INDUSTRY REPRESENTATIVES THAT DEAL WITH THREATS, DETERRENTS, VULNERABILITIES AND PROTECTION MECHANISMS THAT AFFECT THE TELECOMMUNICATIONS INFRASTRUCTURE. IN ADDITION, THE SECRET SERVICE IS ALSO IN THE MIDST OF A MAJOR INTERNATIONAL TRAINING INITIATIVE WHERE WE ARE TRAINING AND INTERACTING WITH INDUSTRY AND LAW ENFORCEMENT REGARDING THE GLOBAL IMPLICATIONS OF TELECOMMUNICATIONS VULNERABILITIES. KNOWING THE PARTICIPANTS AND THEIR CURRENT CONCERNS, APPRECIATING THE TECHNOLOGY AND RECOGNIZING APPROPRIATE AREAS FOR INPUT, HAS BEEN THE STRATEGY OF THE SECRET SERVICE IN OUR INTERACTION WITH THESE PARTIES.

THE SECRET SERVICE CONTINUES TO RESHAPE ITS INVESTIGATIVE MISSION FROM THE ONCE TRADITIONAL REACTIVE POSTURE TO A PROACTIVE RISK ANALYSIS MANAGEMENT PROGRAM, DESIGNED TO TERMINATE REPETITIVE LOSSES IN GOVERNMENT AND INDUSTRY SYSTEMS. WHILE THERE IS STILL THE COMMITMENT TO AGGRESSIVELY INVES-

TIGATE VIOLATIONS, THERE IS ALSO A FOCUS ON PREVENTATIVE MEASURES.

THE PROTECTION OF THAT SYSTEM, AN INTEGRAL PART OUR NATIONAL INFRASTRUCTURE, WILL CONTINUE AS A PRIORITY IN OUR INVESTIGATIVE INITIATIVES.

I THANK THE MEMBERS FOR THEIR TIME AND ALLOWING ME TO EXPRESS OUR VIEWS AND CONCERNS. AT THIS TIME, I WOULD LIKE TO DIRECT YOUR ATTENTION TO A DEMONSTRATION OF SOME OF THE EQUIPMENT THAT IS USED TO FACILITATE THE FRAUD ACTIVITY I HAVE DISCUSSED.

Mr. MCCOLLUM. Thank you very much, Mr. Stenger.

STATEMENT OF ANTHONY R. BOCCHICHIO, ASSISTANT ADMINISTRATOR, OPERATIONAL SUPPORT DIVISION, DRUG ENFORCEMENT ADMINISTRATION

Mr. BOCCHICHIO. Thank you, Mr. Chairman. Before discussing clone telephones and the challenge they pose to law enforcement, I would like to discuss how today's international organized crime syndicates use a sophisticated command and control system to run their drug trafficking organizations within the United States.

The leaders of international groups headquartered in Colombia or in Mexico have at their disposal the most sophisticated telecommunications technology—encrypted phones, faxes, and other communications equipment as well as cloned cellular telephones, enabling them to control organizations which reach into the heartland of America while they, themselves, remain beyond the reach of American justice.

Today a top manager from a Colombian trafficking organization may be as "wired" as any business executive in Silicon Valley. He may use dozens of cell phones each day to avoid tracing, keep records in encrypted files, and coordinate his organization by using computer networks.

As complex as the arrangements of these criminal groups are, U.S. law enforcement agencies have, so far, been able to exploit their communications by using court approved telephone intercepts.

Technology has advanced rapidly and the traffickers have more than kept up. We have begun to see a widespread use of cloned cellular phones.

Cloning cellular phones, also known as cellular-phone piracy, is accomplished by using electronic scanners to record the cell phone numbers as citizens make legitimate calls from their cellular phones. These identification numbers are then programmed or cloned using commercially available software and another telephone instrument. Any calls made with that phone are billed to and traced to a legitimate phone account. Innocent citizens end up with unexplained monthly phone bills.

Once the cell phone pirates have done their work, criminal drug trafficking groups will buy these stolen phone accounts in bulk. Traffickers can communicate using a stock of throwaway phones which are sometimes disposed of after just one call.

Starting in the early 1990s, DEA wire intercept cases began to encounter widespread use of cloned cellular phones by major trafficking organizations, especially Colombian traffickers. The Aldemar Barona organization, a Colombian group responsible for distributing over 1,200 kilograms of cocaine per month relied heavily on cloned phones to coordinate its operations. Ferni Bravo, the

New York cell manager, used cloned phones to conduct business with his workers and to communicate with Barona in Colombia.

In the mid-1990s, several major investigations exposed law enforcement's ability to intercept cloned phones making them less than perfect means of avoiding detection and interception. The more sophisticated drug trafficking groups adopted new and more complicated telecommunications technologies, such as phone banks, prepaid cell phones, prepaid calling cards, and digital telephoning which became available in the mid-1990s.

Many American citizens are still vulnerable to cell phone piracy. Over three million customers still own phones that can be cloned. Today cloned phones are being widely used by surrogate groups in the United States that distribute cocaine, heroin, and methamphetamine for the powerful organized crime groups from Colombia and Mexico. Such groups include Dominican groups, African-American and Puerto Rican street gangs. Nigerian traffickers, who distribute wholesale heroin from Southeast Asia throughout the U.S., have also demonstrated a proclivity for cloned phones.

Recent DEA investigations, which have encountered the use of cloned cellular phones, include the following:

In Philadelphia in 1996, the Javier Usman organization used cloned phones in selling 8 to 12 kilograms of cocaine a week on the streets of Philadelphia supplied by the Cali, Colombia group. The Title III investigation on the cloned phones led to the seizure of 10 kilograms of cocaine.

In the Newark Division, in the Glenn Walker case in 1994, DEA and Secret Service investigators conducted Title III intercepts on cloned cell phones. The telephone company kept the phones in service longer than the usual turnover time, enabling the investigators the time needed to build the case which ended with 30 arrests and the seizure of a kilogram of cocaine and several handguns.

A Baltimore investigation in 1995 involved kilogram quantities of Heroin being brought into New York City by Colombian nationals and distributed in the Baltimore, Maryland area. The Colombians, the middlemen in New York, and the Baltimore distributor used cloned cell phones. The distributor routinely switched phones every few weeks, making it very difficult to identify the new number and maintain the Title III intercepts.

In 1997, the Minneapolis office encountered a methamphetamine distribution organization, connected to sources in Mexico, using cloned phones to manage its distribution in the St. Paul area. The distributors used cell phones cloned from phones belonging to a large business in the area rather than from private individuals. The business was billed for all its cell phones on one statement, and did not notice the increased volume of calls. The traffickers, therefore, continued to use the phone longer than the usual turnaround time, enabling DEA to keep a Title II intercept in place long enough to lead to the seizure of 20 pounds of methamphetamine.

Also in the Chicago Division, another case in 1995 involved a criminal group distributing small amounts of Heroin and kilogram quantities of cocaine from sources of supply in Colombia. The distributors used closed phones for all their communications. The

group also used cloned cell phones to communicate with the sources in Colombia.

By the time investigators identify a violator using a cloned phone and follow the traditional path to a Title III intercept, taking two or three weeks, the violator has moved on to the next cloned phone—thus staying a step ahead of law enforcement. The situation poses a series of problems to drug law enforcement.

We have seen the organized criminal groups from Mexico use cell phones, as well as other sophisticated technology, to communicate with the surrogates they employ in the United States. The groups from Mexico are well known to use violence in their trafficking operations. If these criminal drug gangs have unfettered access to cloned cellular communications, they will be bale to issue with impunity "death warrants" for U.S. law enforcement officers, for witnesses, or for innocent civilians. We rely on intelligence gathered from Title III intercepts of their communications to build a picture of the organizations, identify the individual members, and obtain evidence enabling us to make arrests and take apart whole sections of the criminal organizations at a time.

When the communications of these groups are placed beyond our reach by cloned cellular phones, we will be severely hindered in our ability to make cases against the leadership and U.S.-based infrastructure of these powerful organizations which control the drug trade in our hemisphere.

Finally, the use of cloning and other advanced technology degrades DEA's ability to gather key tactical intelligence needed by the interdiction agencies. Given the volun.e of commercial traffic across the U.S. borders and at U.S. ports of entry, and the sophistication employed by these organized criminal syndicates to smuggle drugs into our country, interdiction is dependent on the intelligence we provide in order to remain effective.

It would be an historic mistake not to stem the growing tide of cell phone piracy. The drug traffickers operating on a global scale today already have at their disposal technology, transportation capabilities and communications equipment which are the envy of many U.S. corporations. Law enforcement capabilities must match the capabilities of major traffickers.

Thank you for the opportunity to testify before you today. I will be happy to answer any questions you may have.

[The prepared statement of Mr. Bocchichio follows:]

PREPARED STATEMENT OF ANTHONY R. BOCCHICHIO, ASSISTANT ADMINISTRATOR, OPERATIONAL SUPPORT, DRUG ENFORCEMENT ADMINISTRATION

Chairman McCollum, Members of the Subcommittee: Thank you for the opportunity to submit my comments for the record on the issue of cloned cellular telephones and their use by the organized international criminal groups that control drug trafficking in our hemisphere. Cloned cellular phones are made by criminals who illegally monitor legitimate cell phone communications, record the identification numbers from these calls, and program them into their own phones, thus making a "clone" of the legitimate phone. The criminals can then use these phones in furtherance of their crimes, with the bill going to the legitimate customer—at least temporarily before the fraud is detected. Before discussing clone phones and the challenge they pose to law enforcement, specifically, it is important to discuss several lessons we have learned over the past several years while investigating international criminal groups—lessons which are shaping our current approach to drug law enforcement at home and overseas.

I would like to provide you and the Members of the Subcommittee with a picture of how today's international organized crime syndicates operate and how they use a sophisticated command and control system to run their drug trafficking organizations within the United States, to distribute the poison they bring into our country. I would like to set the stage with the evolution of drug traffickers' use of technological advances in the past and how we see them using technology now.

I. International Organized Crime Today and Yesterday

Powerful international drug syndicates operate around the world, supplying drugs to American communities, employing thousands of individuals to transport and distribute drugs. The most significant international drug syndicates operating today are far more powerful and violent than any organized criminal groups that we have experienced in American law enforcement. Frequently, these trafficking groups are referred to as "cartels" or "federations"—titles that make these organizations sound like businessmen but that do not capture the true nature of their criminal activities.

Today's major international organized crime drug syndicates are simply the 1990's versions of traditional organized crime mobsters U.S. law enforcement officials have fought since the beginning of this century.

Traditional organized crime leaders operating in places like New York, Chicago or Las Vegas called their business shots on American soil; major traffickers from Colombia and Mexico make decisions from the safety of their headquarters in Cali or Guadalajara. After several decades, law enforcement officers in the U.S. were eventually able to identify, target, arrest, and prosecute mob bosses. Experience has demonstrated that the most effective strategy against organized crime is to direct investigative assets at the leadership of the organized crime syndicates.

There are, however, several key differences between these groups and their one-time domestic counterparts. Members of international groups headquartered in Colombia and Mexico have at their disposal sophisticated technology—encrypted phones, faxes, and other communications equipment as well as cloned cellular telephones. Additionally, they have in their arsenal aircraft, radar, weapons and an army of workers who oversee the drug business from its raw beginnings in South American jungles to the urban areas within the United States. All of this modern technology and these vast resources enable the leaders of international criminal groups to build organizations which reach into the heartland of America, while they themselves remain beyond the reach of American justice.

During the time the Colombian National Police were engaged in their campaign to bring down the Medellin Crime Syndicate, a group of young criminals in Cali, Colombia, led by Miguel Rodrigues Orejuela, his brother Gilberto, and Jose Santa Cruz-Londono were building what was to become the most prolific and successful criminal enterprise in history. Orejuela created an enormous monolithic organization that orchestrated the manufacture of hundreds of tons of cocaine in Colombia, which were moved through the Caribbean and later Mexico, to U.S. markets. However, they were far wealthier, far more dangerous, far more influential, and had a much more devastating impact on the day-to-day lives of the citizens of our country than either their domestic predecessors or the crime families from Medellin.

The Cali bosses were pioneers in using technology to further their goals. They were sophisticated, high tech and proficient in the use of cell phones, pagers, faxes and other conveniences. The cell structure of the monolithic Cali mafia necessitated a complex system of communications to enable the organization's leaders to know in a moment where every kilo of cocaine was located, how much profit was being made, and where and when deliveries would take place. By using cell phones and pagers, the Cali leaders communicated with different segments of the organization, and provided only pieces of information to each segment, reducing the vulnerability of individuals and the entire organization. Today, a top manager from a Colombian trafficking organization may be as "wired" as any business executive in Silicon Valley. He may use dozens of cell phones, often phones that have been cloned, each day to avoid tracing, keep records in encrypted files in a networked data base, and coordinate his organization by using networked computers.

In the early 1990s, the Colombians turned to the less sophisticated and structured Mexican trafficking groups to move their products to growing American drug markets through Mexico and across the U.S. border. These Mexican groups' entrance into the cocaine trade in the United States and their subsequent ascension to power has garnered them enormous wealth and a demonstrative expansion in their spheres of influence. The organized criminal groups from Mexico now control virtually all cocaine sold in the Western half of the United States and, for the first time, we are seeing a concerted effort on their part to expand into the lucrative East Coast market.

As complex as these communications arrangements of these criminal groups were, U.S. law enforcement agencies have been able to exploit their communications by using court approved telephone intercepts. With the top leadership of these organizations in hiding beyond the reach of U.S. law enforcement, we directed our resources at their organizational structure, and their transportation and distribution elements in the United States.

Technology has advanced rapidly and the traffickers have more than kept up. As long as there is technology, the world's most powerful drug traffickers will find ways to conduct their business, even from jail. Recently the Colombian National Police (CNP) learned that Miguel and Gilberto Rodriguez Orejuela were conducting business over cell phones, the Internet and faxes from their prison cells. (The CNP raided offices of private telecommunications switching centers in Bogota where the jailed leaders had bribed a clerk to patch their calls to anywhere in the world).

II. Organized Crime's Surrogates in the United States

The international drug trafficking syndicates cannot operate effectively without an infrastructure in the United States composed of high level managers, transporters, accountants, communications experts, storage experts and enforcers. The Colombian traffickers, and to a large extent, the traffickers from Mexico have established bases of operations in major U.S. cities, and rely on an intricate network of cells, similar to international terrorist organizations in the way they are insulated from each other. Cell managers maintain close communication with syndicate leaders in Colombia and Mexico, and are in some sense, the "foreign service" of these drug organizations, representing the syndicate's interests abroad.

These surrogates who control operations throughout the U.S. engage in complicated efforts to avoid having their telephone communications vulnerable to legal wiretaps. They buy legitimate and cloned cell phones in lots of 10–20, which are used for a few weeks or even days and then quickly discarded and replaced in order to evade wiretaps by moving from phone to phone more quickly than law enforcement could keep up. Pagers are used to communicate locations through codes, not phone numbers, which could be incriminating. Pay phones are frequently used instead of their private line phones which are likely to be tapped. The sight of a drug trafficker stuffing rolls of quarters into pay phones during long distance calls to Colombia is common. Sophisticated codeword systems were developed to communicate times and locations for drug deliveries and money pickups, as well as key telephone numbers which could be used for incoming calls. We are able to exploit all these communications to some degree by using court approved wiretap intercepts.

III. The Technology of Cloned Cellular Phones

Today's international drug trafficking organizations are the wealthiest, most powerful, and most ruthless organized crime organizations we have ever faced. We know from our investigations that they utilize their virtually unlimited wealth to purchase the most sophisticated electronic equipment available on the market to facilitate their illegal activities. We have begun to see that this includes widespread use of cloned cellular telephones. Aside from the crimes which may be committed once the phones are cloned, fraud from cloning is estimated to cost the cellular industry more than $1 million every day. Costs are expected to rise by 40% per year unless effective countermeasures are taken. Not only are the customers whose phones are cloned inconvenienced, but every customer is hurt as companies raise rates to cover losses to fraud.

Cloning cellular phones, also known as cellular-phone piracy, is accomplished by staking out high-traffic areas, such as airports, bridges, tunnels or office complexes, and using electronic scanners to record the cell phone identification numbers, as citizens in the area make legitimate calls with their phones. Technically, these numbers are the cellular phone number, or mobile identification number (MIN), and the electronic serial number (ESN). These identification numbers are then programmed, or "cloned," using commercially available software, on another telephone instrument. This process, although seemingly complex, actually takes only about a minute for the technically skilled criminal to accomplish.

Legally, this procedure is a variety of counterfeit fraud. Any calls made with that phone are billed to, and traced to, the original, legitimate phone account. Innocent citizens end up with huge, unexplained monthly phone bills. A related form of counterfeit fraud is the use of "tumbler phones," in which the criminals switch the MIN and ESN combinations in their phones at will. These MIN and ESN combinations may enable the cell phone to penetrate some switching systems, giving the criminals free cell phone service, but without the theft from legitimate customers. Because of the continuously changing MIN and ESN numbers, law enforcement will not likely be able to trace tumbler phones.

The newest and most insidious form of cell phone counterfeit is the "Tumbler-Clone." This method shifts through the numerous legitimate MIN and ESN pairs, which have been previously pirated, programed into the phone, using a different pair at each call. At the switch, it will appear that a different legitimate phone makes each call. This method has not yet been a proven success, and is not yet widespread.

A cell phone theft method similar to counterfeit fraud is subscription fraud. This method requires someone on the inside of a telecommunications carrier unknowingly or willingly allowing a customer to present false or altered identification and receive activated cellular service. The fraudulent customer then enjoys free cell service, at least until the carrier terminates service for non- payment.

Once the cloned phone is in use by the criminals, the time until the clone is detected by the carrier or by the customer can vary. The carriers have programmed their systems to recognize high volume calls to key cities, international calls, or excessive calling patterns, tipping them off to a potential fraud in process. The systems can also recognize the legitimate phone apparently operating in two geographical parts of the system at the same time, a physical impossibility indicating the presence of a clone phone in operation. Otherwise, the first warning may be when a customer receives a huge phone bill, and complains to the carrier. The carrier can shut off the clone phone instantly, and customers can have the fraudulent bills credited by the carrier. The carrier, however, has already incurred the cost.

Once the cell phone pirates have done their work, through whichever method, other criminal groups will buy these stolen cell phone accounts in bulk from the individuals or organizations doing the cloning. This process is so simple that traffickers can communicate using a stock of "throw-away" phones, which are sometimes disposed of after just one call in an effort to stay even further ahead of law enforcement efforts to trace them. Put another way, traffickers rotating phones in this manner basically thwart efforts at intercepting their phone conversations. Not being able to intercept the command and control communications of a trafficking frustrates one of our most valuable investigative tools.

We have seen these criminals use cloned cell phones widely throughout their trafficking organizations and as part of their compartmentalization in international trafficking of drugs. These phones are used to issue orders between the leaders of transportation and distribution cells regarding the movement of thousands of tons of cocaine from Colombia and Mexico on the streets of the United States. Clone phones are more widely used by criminals in the next layer down in the cocaine and other drug trafficking organizations in the United States, to communicate between themselves.

Starting in the early 1990s, DEA wire intercept cases began to encounter widespread use of cloned cellular phones by major trafficking organizations, especially Colombian traffickers. The Aldemar Barona organization, a Colombian group responsible for distributing over 1,200 kilograms of cocaine per month relied heavily on clone phones to coordinate its operations. Ferni Bravo, the New York cell manager, and his workers used cloned cellular phones to conduct their day-to-day business and to avoid interception. Bravo always used cloned cell phones to communicate with Barona in Colombia, to receive information on arriving shipments of cocaine and directions on returning drug proceeds to Colombia. During this investigation, Bravo changed cloned phones every week or two, making it extremely difficult to identify his new phones in order to obtain a Title III warrant before he moved on to the next phone.

In the period from 1993 to 1995, the problem of cell phone cloning in New York was at its peak. During this time, two U.S. Secret Service agents were detailed to DEA's New York Division to work cases jointly, so as to more efficiently direct law enforcement resources against the problem. The increased use of cloned cell phones continued throughout 1995, when the Colombians switched to other means of communications, which I will detail below.

During this same time, several major investigations exposed law enforcement's ability to intercept cloned phones, making them a less than perfect means of avoiding detection and interception. The more sophisticated trafficking groups adopted new and more complicated telecommunications technologies which became available in the mid-1990s. Law enforcement investigations of cell phones used for criminal purposes, in addition to telephone company efforts at fraud management, have decreased the use of cloned phones by sophisticated trafficker organizations. Recent technologies such as authentification, radio frequency fingerprinting, and the development of the digital Personal Communications System (PCS), as an attractive alternative, have decreased the opportunities for cloning. Many American citizens are still vulnerable to cell phone piracy, however,—over three million customers still

own phones that can be cloned. Some of the new communications technologies, which the sophisticated traffickers adopted, include the following:

- *Phone arcades or Phone Banks:* These are essentially a storefront business with a dozen or so small phone booths. A customer pays the store clerk, in cash, for the calls made—based on duration and destination. Although Title III investigations have been conducted against this activity, the very nature of the operation—in which the caller remains anonymously behind a cash transaction with the clerk—has meant that the investigations have not produced significant results.
- *Pre-paid Cellular Phones:* These so called "Can Call" phones can be purchased in vending machines or from distributors, each one already supplied with a pre-paid amount of calling time. Use of this method makes such calls extremely difficult to trace, as the calls take place *after* payment is made.
- *Pre-paid Calling Cards:* These cards can be purchased from vending machines, in convenience stores, or even through cereal box promotions or through airline magazines. The cards can then be used by traffickers to place calls that, because of their volume and easy accessability, are extremely difficult for law enforcement to trace.
- *Digital Cellular Phones:* Because these phones employ transmissions of a string of digits, rather than an analog voice signal, requiring digital equipment to receive or intercept, these phone provide a significant measure of privacy to the caller. They are the most secure form of communications available on the open market, especially when coupled with encryption devices. These digital phones are less likely to be cloned than older, analog phones. Until the networks become fully digital, the "network handshake" that sets up a call from a digital phone to an analog phone will still be conducted in analog mode. This portion of the transmission may still be cloned.

Today, in 1997, cloned phones are being widely used by surrogate groups who distribute cocaine, heroin, and methamphetamine for the powerful organized crime groups from Colombia and Mexico. Such groups include Dominican groups, African-American and Puerto Rican street gangs. Nigerian traffickers, who distribute wholesale heroin from Southeast Asia throughout the U.S., have also demonstrated a proclivity for cloned phones.

DEA Divisions across the country have had several investigations in the recent past in which we encountered the use of cloned cellular phones—showing how wide spread this problem is. These traffickers are able, when using cloned phones to avoid tracing or interception, to pass orders on movements, places and times of delivery, and mode of transportation for cocaine, heroin, and methamphetamine. The traffickers have a reasonable certainty that U.S. law enforcement will temporarily not be able to intercept their communications while we catch up with their rapid shifting of phones.

- In Philadelphia in 1996, the Javier Usman organization used cloned phones to avoid detection by law enforcement in conducting his operations that sold 8–12 kilograms of cocaine a week on the streets of Philadelphia. The cocaine was supplied by a group in Cali, Colombia. The Usman organization used threats and intimidation to protect their territory. The Title III investigation on the cloned phone led to seizure of 10 kilograms of cocaine.
- The Newark Division had the Brian Thomas Elliot case in 1996, where the violator had a cloning apparatus and used four different cloned phones during the investigation. In the Glenn Walker case in 1994, DEA and Secret Service investigators conducted Title III intercepts on three cloned cell phones used by the violators, who hired another individual to do the cloning for them. The traffickers threw away the first phone before the intercept was initiated. The telephone company kept the next two phones in service for more than a month, longer than the usual turnover time, enabling the investigators the time needed to build the case. The investigation ended with 30 arrests, and seizure of a kilogram of cocaine and several handguns. DEA seized 20 cloned cell phones and a hundred cloned beepers, along with the cloning equipment, from the cloning technician.
- A Baltimore investigation in 1995 involved kilogram quantities of Heroin being brought into New York by Colombian nationals, and distributed in the Baltimore, Maryland area. The Colombians, the middlemen in New York, and the Baltimore distributor used cloned cell phones, The distributor routinely switched phones every few weeks, making it very difficult to identify the new number and maintain the Title III intercepts. Documenting the probable cause to show that the new phone would be used for drug operations was an intensive effort.

- In the Chicago Division in 1997, the Minneapolis office encountered a methamphetamine distribution organization, connected to sources in Mexico, using clone phones to manage its operations in the St. Paul area. More than 30 pounds of methamphetamine a month was being transported, through California, to St. Paul, where it was distributed by Mexican-American gangs. The distributors used cell phones cloned from phones belonging to a large business in the area, rather than from private individuals. The business was billed for all its cell phones on one statement, and did not notice the increased volume of calls on a few of its phones. The traffickers, therefore, continued to use each phone for a month or more, longer than the usual turnaround time, enabling DEA to keep a Title III intercept in place long enough to make a case leading to seizure of 20 pounds of methamphetamine.
- Also in the Chicago Division, another case in 1995 involved a criminal group in the Chicago area distributing small amounts of Heroin and kilogram amounts of Coke from sources of supply in Colombia. The distributors used clone phones for all their communications, both coordinating their drug operations and their personal conversations as well. In fact, some of the members of the group did not even own legitimate phones. The group also used cloned cell phones to communicate with the sources in Colombia. The cell phones were cloned by a violator working with the trafficking group, who guaranteed that the clone phones bought from him would be good for a minimum period of service before being detected and shut off by the carrier, or he would issue another cloned cell phone with the same guarantee.

IV. The Problems Posed to Law Enforcement by Cloned Cellular Phones

Like other technologies, the development of cellular telephone communications in the 1980s threatened to out pace law enforcement's ability to adjust to the changing environment. Law Enforcement met the technical challenge, and continues to meet it through CALEA and related efforts to keep pace with digital telephony. Cell phone piracy shows that criminals have taken the next logical step in technology. They can communicate with each other with flexibility, as they have long done, but now they can do so more anonymously and can remain better insulated from detection. Provided the turnover rate, at which they move to a new phone and discard an old one, is less than 2–3 weeks, they can beat the average amount of time it generally takes to obtain a court ordered intercept warrant. By the time investigators identify a violator using a cloned phone and follow the traditional path to a Title III intercept, the violator has moved on to the next cloned phone—thus staying a step ahead of the law.

We have seen the organized criminal groups from Mexico use cell phones, as well as other sophisticated technology, to communicate with the surrogates they employ in the United States. If these criminal drug gangs have unfettered access cloned cellular communications, with which we in law enforcement cannot keep pace, then they will be able to do more than issue orders for transporting drugs which we cannot easily foil. We have seen violence erupt on both sides of the U.S.-Mexico border in recent years. With presumably private conversations, the traffickers will be able to issue with impunity "death warrants" for U.S. law enforcement officers, for witnesses, or for innocent civilians. They will be able to continue their reign of drug terror in the United States—a very immediate, bloody threat to the national security in addition to the threat from the drugs they sell.

In addition to the potential for violence, cloning cell phones poses a strategic problem for DEA in its focus on the communications of command and control functions of international drug trafficking organizations. We rely on the intelligence gathered from Title III intercepts of their communications to build a picture of the organizations, identify the individual members, and obtain evidence enabling us to make arrests and take apart whole sections of the criminal organizations at a time—as we did recently in Operations Limelight and Reciprocity. These investigations have clearly demonstrated the value of this approach. To the extent that the communications of these groups are placed beyond our reach by cloned cellular phones, and other technological advances, such as encryption and digital telephony, which change at a rate with which we cannot keep up, we will be severely hindered in our ability to make cases against the leadership and U.S.-based infrastructure of these powerful organizations which control the drug trade in our hemisphere.

Finally, the use of cloning and other advanced technology degrades DEA's ability to gather key tactical intelligence needed by the interdiction agencies. Given the volume of commercial traffic across the U.S. borders and at U.S. ports of entry, and the sophistication employed by these organized criminal syndicates to smuggle drugs into our country, interdiction is dependent on the intelligence we provide in order to remain effective.

V. Conclusion

It would be an historic mistake not to stem the growing tide of cell phone piracy. The drug traffickers operating on a global scale today already have at their disposal technology, transportation capabilities and communications equipment which are the envy of many U.S. corporations. Law enforcement capabilities must match the capabilities of major traffickers. However, with rapid changes in technology, such as cellular communications systems, and encrypted equipment, and with assistance from U.S. manufacturers, law enforcement is facing a difficult situation which, unless quickly addressed, will even more seriously impede our ability to do business in just a few, short years.

Thank you for the opportunity to testify before you today. As always it has been a pleasure, and I will be happy to answer any questions you may have.

Mr. MCCOLLUM. Thank you very much, Mr. Bocchichio. Mr. Navarrete, you may proceed with your testimony.

STATEMENT OF JOHN NAVARRETE, DEPUTY ASSISTANT DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Mr. NAVARRETE. Thank you, Mr. Chairman. Mr. Chairman and members of the Subcommittee on Crime, I would like to thank you for providing me with this opportunity to discuss with you the crime of illegally cloned cellular telephones and the impact that the proliferation of these devices has on law enforcement.

Cellular telephone fraud is a rapidly expanding crime problem which seriously affects the public, the cellular telephone industry, and law enforcement. The crime usually begins with the victimization of the individual cellular telephone users and ends with the loss of millions of dollars by cellular telephone companies. However, there are many law enforcement concerns and crime problems between these beginning and end points. Today, I hope to share some of these with you.

Cellular telephone "cloning," as already explained or testified to, occurs when an unauthorized person reprograms a cellular telephone with the electronic identification data from a different, valid cellular telephone of a legitimate, unsuspecting cellular phone customer. Once the phone has been cloned, there are two phones with the same electronic identity, one legal and one illegal. Calls made from the illegal, cloned cellular phone appear to be coming from the legitimate phone and are billed to the account of the legitimate customer.

The first victims of this crime are the legitimate customers who are inconvenienced by having to change cellular telephone numbers and have their phones reprogrammed. There are also potentially more serious consequences for the legitimate customer: under certain circumstances, they could be denied access to the cellular telephone system while the cloned telephone is being used. If this should occur during an emergency, it could result in the inability to summon police or medical help.

At the other end of the crime are the cellular telephone companies that suffer the losses due to the fraudulent calls made on the cloned telephones. Cellular telephone industry sources estimated that cellular telephone fraud cost the industry as much as $650 million in 1995. While the legitimate cellular telephone customer and the cellular telephone company are clearly victims of this crime, the problems caused by cellular telephone cloning do not stop there.

Cellular telephone fraud is a complex and sophisticated crime which often involves or facilitates other criminal activities. A cloned cellular phone has the same electronic identity as the legitimate phone. Therefore, calls made on cloned cell-phones cannot be traced. Tracing or other investigation leads only to the innocent owner of the legitimate telephone. The fact that calls made from cloned cell-phones are untraceable is most appealing to drug traffickers and other criminals seeking to hide from law enforcement.

In addition to conferring a cloak of anonymity, use of cloned cellphones by criminals has other benefits. First, cloned cell-phones are a bargain for the criminal. In most metropolitan areas, a cloned phone can be obtained for a few hundred dollars. Some cell-phone cloners will even guarantee a phone for 30 days and will re-clone the phone if the service is terminated before 30 days have elapsed. Regardless of how long the cloned phone is active, the typical call volume of an illegal cloned phone user is such that the value of the service stolen quickly exceeds the amount paid for the phone and the calls essentially become free.

Secondly, cloned cell-phones are usually sold on a cash basis with no credit checks or background references. Thus, criminals can easily acquire them with no paper trail detectable by law enforcement. This ease of anonymous acquisition, coupled with the untraceableness of the calls, makes the proliferation of cloned cellphones a serious threat to law enforcement at all levels.

I will now give you a couple of examples of how we confront this problem: In some fast paced situations such as a kidnapping investigation, these problems can endanger the lives of innocent victims. The FBI recently investigated a kidnapping in Los Angeles where a Mexican, drug organization operating out of Tijuana, kidnapped the son of a local Los Angeles drug dealer who owed them a debt. The victim, a 14-year old boy, was kidnapped from his home in Seattle, Washington. The boy was transported to the Los Angeles area where kidnappers began to negotiate a ransom with the father using a cellular telephone which had been cloned with a cell-phone number out of Seattle. As a result, there were substantial time delays while telephone companies in Los Angeles, where the phone was being used, and Seattle, from which the legitimate number had been cloned, tried to identify where the phone was located.

At one point, the telephone companies mistakenly identified a residence address as the point of origin for the calls because the cloned cell-phone number had previously been a hard-wired number and had only recently been assigned to a cellular telephone in Seattle. FBI agents responded to the address only to find startled residents and no kidnapping victim. Fortunately, the telephone companies ultimately identified the cloned number and the FBI agents were able to conduct an emergency Title III interception of the ransom calls as well as determine the whereabouts of the kidnappers.

The child was safely recovered, however, the delays and difficulties encountered because of the kidnappers use of a cloned cellphone significantly increased the danger to the kidnap victim.

Violent criminals are not the only ones taking advantage of illegally cloned cell-phones. White collar criminals also use these devices. Over the past 2 years, the FBI in Los Angeles also inves-

tigated two Eastern European/Russian organized crime groups involved in fuel excise tax evasions, resulting in several million dollars lost to the Department of Transportation. The subjects were also involved in heroin trafficking.

During the course of the investigation, the targets used three cloned cellular telephones. In order to conduct court authorized wiretaps, agents had to repeatedly research and prepare additional affidavits to accommodate the continual reprogramming of the cloned cellular telephones. This laborious task not only diverted agents' investigative efforts but presented potential safety issues for undercover operatives.

On a Friday during which an undercover purchase of a kilogram of heroin from a subject had been scheduled, the subject reprogrammed his cloned cell-phone. Agents delayed the drug transaction to the following Monday in order to prepare an affidavit and obtain a court order for the new cloned phone over the weekend.

On the following Monday, just prior to the drug transaction, the subject reprogrammed his cloned cellular phone again and the agents were unable to have telephone coverage for the transaction, placing the undercover operative at much greater risk. The agents overcame these challenges to build a successful case. And as a sideline, to date, 22 of the 26 individuals indicted have pled guilty to charges ranging from racketeering, heroin trafficking, prostitution, extortion , and money laundering, to also include fuel excise tax evasion. There have also been millions of dollars in fines, forfeitures and restitution. The same situations are encountered investigating street gangs and, as already pointed out, in drug investigations.

There is another hidden cost of conducting court authorized wiretaps of cloned cell-phones. Cellular telephone companies normally will immediately shut off services when it becomes known that a cell-phone has been cloned. This usually occurs when the legitimate customer receives a bill containing unauthorized call charges and notifies the cell-phone company. When law enforcement identifies a cloned cell-phone as a wiretap target, the law enforcement agency must pay the cellular telephone company for all of the unauthorized call charges of the criminal in order to keep the cloned cell-phone from being shut off. And I may add that we have investigations that we have been up on wires for as long as 7 to 12 months and we pay the bills.

From the above examples, it is clear that the proliferation of cloned cell-phones has not only altered the landscape for court authorized, law enforcement wiretaps but has created many other challenges for law enforcement. The use of cloned cellular telephones by the subjects of criminal investigations can result in delays and confusion in the correlation of intercepted information and identification of criminal subjects, increased danger to crime victims and law enforcement officers, and the ultimate concealment of criminal activity. Valuable intercepts are lost because criminals can change cloned cell-phone numbers faster than the lengthy wiretap approval process can react.

When cloned cellular telephones are being used, it is no longer practical for law enforcement to identify a specific telephone being used by the targeted criminal. Cloned cell-phones are so readily

and cheaply available that criminals can change cloned cellular telephones as easily as changing locations.

Congress, in enacting Title III, properly recognized the fact that dangerous criminals routinely use our Nation's telecommunications networks to carry out their criminal activities—activities which threaten the personal safety and economic well-being of the innocent, law abiding citizens of our nation. Title III wiretaps are an extremely important and effective technique used only in investigations of the most serious crimes. In many cases, there is no substitute for court-ordered interceptions in gathering evidence, preventing crimes, solving crimes, and bringing the violent to justice. During the past 14 years, the use of authorized, court-ordered interceptions has directly resulted in the conviction of over 26,000 dangerous felons.

Criminals' easy access to cloned cellular telephones must not be allowed to erode the ability of law enforcement to effectively use the tools provided by Title III. There are two important things that the Congress can do to help:

First, the cloning problem could be dramatically reduced if cellular telephone manufacturers were required to produce cellular telephones that are not so easily reprogrammable. If one considers the matter, there is no need for cellular telephones to be reprogrammable outside of authorized company service centers. Law abiding cellular telephone users are not constantly reprogramming their cellular telephones nor do they want to; it is only the criminal community that is engaged in this activity.

Secondly, statutory provisions for multi-point wiretap authority need to reflect the realities of the illegal technology now readily available not only to the most sophisticated criminals but to virtually any criminal on the street. The current language under Section 2518(11) of Title 18, United States Code, should be modified so that the legal standards for interception of wire or electronic communications are in harmony with existing language regarding the interception of oral communications.

There is currently a disparate standard where authority for a multi-point oral intercept requires only a demonstration by law enforcement and a judicial finding that specifying a particular meeting place is not practical while multi-point authority for wire or electronic interception requires a demonstration and judicial finding that the criminal is intentionally attempting to thwart surveillance. Bringing the legal standards for wire and electronic interceptions into harmony with existing standards for oral intercepts would eliminate the needless, cumbersome, and often life-threatening circumstances found today where law enforcement officers and prosecutors go through the lengthy Title III application process only to have their efforts rendered useless by the subject reprogramming a cloned cellular phone.

Mr. Chairman, thank you and at this time I will be happy to answer any questions you or the members of the Subcommittee may have.

[The prepared statement of Mr. Navarrete follows:]

PREPARED STATEMENT OF JOHN NAVARRETE, DEPUTY ASSISTANT DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Mr. Chairman and Members of the Subcommittee on Crime, I would like to thank you for providing me with this opportunity to discuss with you the crime of illegally cloned cellular telephones and the impact that the proliferation of these devices has on law enforcement.

Cellular telephone fraud is a rapidly expanding crime problem which seriously affects the public, the cellular telephone industry, and law enforcement. The crime usually begins with the victimization of the individual cellular telephone users and ends with the loss of millions of dollars by cellular telephone companies. However, there are many law enforcement concerns and crime problems between these beginning and end points. Today, I hope to share some of these with you and the Members of this Subcommittee.

Cellular telephone "cloning" occurs when an unauthorized person reprograms a cellular telephone with the electronic identification data from a different, valid cellular telephone of a legitimate, unsuspecting cellular phone customer. Once the phone has been cloned, there are two phones with the same electronic identity, one legal and one illegal. Calls made from the illegal, cloned cellular phone appear to be coming from the legitimate phone and are billed to the account of the legitimate customer.

The first victims of this crime are the legitimate customers who are inconvenienced by having to change cellular telephone numbers and have their phones reprogrammed. There are also potentially more serious consequences for the legitimate customer: under certain circumstances, they could be denied access to the cellular telephone system while the cloned telephone is being used. If this should occur during an emergency, it could result in the inability to summon police or medical help. At the other end of the crime are the cellular telephone companies that suffer the losses due to the fraudulent calls made on the cloned telephone. Cellular telephone industry sources estimated that cellular telephone fraud cost the industry as much as $650 million in 1995. While the legitimate cellular telephone customer and the cellular telephone company are clearly victims of this crime, the problems caused by cellular telephone cloning do not stop there.

Cellular telephone fraud is a complex and sophisticated crime which often involves or facilitates other criminal activities. A cloned cellular phone has the same electronic identity as the legitimate phone. Therefore, calls made on cloned cellphones cannot be traced. Tracing or other investigation leads only to the innocent owner of the legitimate telephone. The fact that calls made from cloned cell-phones are untraceable is most appealing to drug traffickers and other criminals seeking to hide from law enforcement.

In addition to conferring a cloak of anonymity, use of cloned cell-phones by criminals has other benefits. First, cloned cell-phones are a bargain for the criminal. In most metropolitan areas, a cloned phone can be obtained for a few hundred dollars. Some cell-phone cloners will even guarantee a phone for 30 days and will re-clone the phone if the service is terminated before 30 days has elapsed. Regardless of how long the cloned phone is active, the typical call volume of an illegal cloned phone user is such that the value of the service stolen quickly exceeds the amount paid for the phone and the calls essentially become free.

Secondly, cloned cell-phones are usually sold on a cash basis with no credit checks or background references. Thus, criminals can easily acquire them with no paper trail detectable by law enforcement. This ease of anonymous acquisition, coupled with the untraceableness of the calls, makes the proliferation of cloned cell-phones a serious threat to law enforcement at all levels.

Cloned cell-phones present significant problems to law enforcement in the identification and apprehension of violent criminals. In some fast paced situations such as a kidnapping investigation, these problems can endanger the lives of innocent victims. The FBI recently investigated a kidnapping in Los Angeles where a Mexican drug organization operating out of Tijuana kidnapped the son of a local Los Angeles drug dealer who owed them a debt. The victim, a 14 year old boy, was kidnapped from his home in Seattle, Washington. The boy was transported to the Los Angeles area where kidnappers began to negotiate a ransom with the father using a cellular telephone which had been cloned with a cell-phone number out of Seattle. As a result, there were substantial time delays while telephone companies in Los Angeles, where the phone was being used, and Seattle, from which the legitimate number had been cloned, tried to identify where the phone was located. At one point, the telephone companies mistakenly identified a residence address as the point of origin for the calls because the cloned cell-phone number had previously been a hard-wired number and had only recently been assigned to a cellular tele-

phone in Seattle. FBI agents responded to the address only to find startled residents and no kidnapping victim. Fortunately, the telephone companies ultimately identified the cloned number and FBI agents were able to conduct an emergency Title-III interception of the ransom calls as well as determine the whereabouts of the kidnappers. The child was safely recovered, however, the delays and difficulties encountered because of the kidnappers use of a cloned cell-phone significantly increased the danger to the kidnap victim.

Violent criminals are not the only ones taking advantage of illegally cloned cellphones. White collar criminals also use these devices. Over the past two years, the FBI Los Angeles government fraud squad has been investigating two Eastern European/Russian organized crime groups involved in fuel excise tax evasion, resulting in several million dollars lost to the Department of Transportation. The subjects were also involved in heroin trafficking. During the course of the investigation, the targets used three cloned cellular telephones. In order to conduct court authorized wire-taps, agents had to repeatedly research and prepare additional affidavits to accommodate the continual reprogramming of the cloned cellular telephones. This laborious task not only diverted agents investigative efforts but presented potential safety issues for undercover operatives. On a Friday during which an undercover purchase of a kilogram of heroin from a subject had been scheduled, the subject reprogrammed his cloned cell-phone. Agents delayed the drug transaction to the following Monday in order to prepare an affidavit and obtain a court order for the new cloned phone over the weekend. On the following Monday, just prior to the drug transaction, the subject reprogrammed his cloned cellular phone again and the agents were unable to have telephone coverage for the transaction, placing the undercover operative at much greater risk. The agents overcame these challenges to build a successful case. To date, 22 of the 26 individuals indicted have pled guilty to charges ranging from racketeering, heroin trafficking, prostitution, extortion, and money laundering, to fuel excise tax evasion. There have also been millions of dollars in fines, forfeitures and restitution.

Cloned cell-phones clearly present serious obstacles to law enforcement's use of court authorized wire-taps on criminals. In many cases, the criminal is using a cloned cell-phone simply because it is an easy and low cost way to communicate. However, some sophisticated criminals have learned from law enforcement's successful use of court authorized wire-taps to dismantle criminal enterprises and are now using cloned cell-phones to thwart law enforcement efforts. These criminals maximize the anonymity conferred by cloned cell-phones by regularly acquiring new cloned cell-phones and discarding their old ones after only a few days of use. Regardless of the motivation, the use of cloned cell-phones by criminals seriously hinders law enforcement's ability to conduct court authorized electronic surveillance.

A recent FBI investigation of an extremely violent gang in Los Angeles, the Grape Street Crips, illustrates the challenges of monitoring cloned cellular phones used by criminals. A critical component of this gang investigation involved wire-taps on key gang leaders who were using cloned cell-phones. During the seven months of wire-tap coverage on the clone telephones used by the gang leaders, agents had to prepare at least twelve different affidavits and apply for twelve separate court orders to accommodate the continual reprogramming of the gang leaders cloned cellular telephones to different numbers. In fact, three affidavits were written, but not used, because the telephones were reprogrammed before approvals for wire-taps could be obtained. There was a significant waste of time and resources attempting to identify the subscriber and prepare necessary probable cause to justify a Title-III interception only to have to abandon the process in pursuit of another telephone number every few days. Despite effort required to overcome the obstacles presented by the gang leaders' use of cloned cell-phones, the investigation was very successful. It identified an extensive interstate drug trafficking network that extended throughout the country including Los Angeles, Cleveland, Memphis, Minneapolis and Mississippi. The investigation resulted in the indictment of 57 subjects nationwide, numerous seizures of cocaine hydrochloride, cocaine base, crack cocaine and the seizure of over $516,000 in U.S. currency.

An FBI investigation in Ft. Worth, Texas involving multiple Title-III interceptions directed at a drug trafficking organization provides an example of another type of difficulty presented to law enforcement agencies by cellular cloning. In this case, telephone trap and trace procedures were being used to identify the cellular phones from which calls to a known subject were being made. The trap and trace identified a cellular telephone number used on several occasions by one drug trafficker to contact the subject. Investigation determined this number to be the personal cellular telephone number of a mid-level police official. After extensive research with the cellular service provider, FBI agents were able to verify that the calls were being placed from a cloned telephone and not the cellular telephone of the police official.

Until this was resolved, it caused a diversion of resources and investigative focus to consider the possibility of public corruption, which did not, in fact, exist in the case.

There is another hidden cost of conducting court authorized wire-taps of cloned cell-phones. Cellular telephone companies normally will immediately shut off service when it becomes known that a cell-phone has been cloned. This usually occurs when the legitimate customer receives a bill containing unauthorized call charges and notifies the cell-phone company. When law enforcement identifies a cloned cell-phone as a wire-tap target, the law enforcement agency must pay the cellular telephone company for all of the unauthorized call charges of the criminal in order to keep the cloned cell-phone from being shut off.

From the examples above, it is clear that the proliferation of cloned cell-phones has not only altered the landscape for court authorized, law enforcement wire-taps but has created many other challenges for law enforcement. The use of cloned cellular telephones by the subjects of criminal investigations can result in delays and confusion in the correlation of intercepted information and identification of criminal subjects, increased danger to crime victims and law enforcement officers, and the ultimate concealment of criminal activity. Valuable intercepts are lost because criminals can change cloned cell- phones numbers faster than the lengthy wire-tap approval process can react.

When cloned cellular telephones are being used, it is no longer practical for law enforcement to identify a specific telephone being used by the targeted criminal. Cloned cell-phones are so readily and cheaply available that criminals can change cloned cellular telephones as easily as changing locations.

Congress, in enacting Title-III, properly recognized the fact that dangerous criminals routinely use our nation's telecommunications networks to carry out their criminal activities—activities which threaten the personal safety and economic well-being of the innocent, law abiding citizens of our nation. Title-III wire-taps are an extremely important and effective technique used only in investigations of the most serious crimes. In many cases, there is no substitute for court-ordered interceptions in gathering evidence, preventing crimes, solving crimes and bringing the violent to justice. During the past 14 years, the use of authorized, court-ordered interceptions has directly resulted in the conviction of over 26,000 dangerous felons.

Criminals' easy access to cloned cellular telephones must not be allowed to erode the ability of law enforcement to effectively use the tools provided by Title-III. There are two important things that the Congress can do to help.

First, the cloning problem could be dramatically reduced if cellular telephone manufacturers were required to produce cellular telephones that are not so easily reprogrammable. If one considers the matter, there is no need for cellular telephones to be reprogrammable outside of authorized company service centers. Law abiding cellular telephone users are not constantly reprogramming their cellular telephones nor do they want to; it is only the criminal community that is engaged in this activity.

Secondly, statutory provisions for multi-point wire-tap authority need to reflect the realities of the illegal technology now readily available not only to the most sophisticated criminals but to virtually any criminal on the street. The current language under section 2518 (11) of Title 18, United States Code, should be modified so that the legal standards for interception of wire or electronic communications are in harmony with existing language regarding the interception of oral communications. There is currently a disparate standard where authority for a multipoint oral intercept requires only a demonstration by law enforcement and a judicial finding that specifying a particular meeting place is not practical while multipoint authority for wire or electronic interception requires a demonstration and judicial finding that the criminal is intentionally attempting to thwart surveillance. Bringing the legal standards for wire and electronic interceptions into harmony with existing standards for oral intercepts would eliminate the needless, cumbersome and often life-threatening circumstances found today where law enforcement officers and prosecutors go through the lengthy Title-III application process only to have their efforts rendered useless by the subject reprogramming a cloned cellular phone.

Mr. Chairman, at this time I will be happy to answer any questions you or the Members of the Subcommittee may have.

Mr. MCCOLLUM. Thank you very much, Mr. Navarrete. We appreciate all of your testimony.

Mr. Stenger, I understand we have a demonstration which you are going to present to us.

Mr. STENGER. Yes, that is correct. Agent Riley will put on a demonstration of how the cloning process takes place. Just a little background on her: In the early '90s, we established a telecommunications squad in Miami because of the problem that existed there and Agent Riley was the lead investigator, so she has accumulated a whole wealth of knowledge. We were wise enough to realize that it was time for her to leave the good life of Miami and come up here to Washington.

Mr.MCCOLLUM. We always enjoy getting a Floridian up here. Please, Agent Riley, come forward and show us your demonstration.

Ms. RILEY. Thank you, Mr. Chairman.

Mr. MCCOLLUM. You are welcome.

Ms. RILEY. What I would like to demonstrate for you this morning is some of the equipment that we have actually seized from some of the fraud operations that have been completed and adjudicated by the Secret Service and to show you how easy it is to actually steal someone's account number and clone that into another cellular telephone.

I would like to show you some equipment that we have had running for about an hour now and this is one of the popular methods being used to actually steal innocent individuals' cellular account numbers before they are cloned into other cellular telephones. On top there is the display from a scanner that we have running. The scanner was actually just a routine scanner that can be purchased from any commercial location but then it has been modified, so instead of intercepting voice it can intercept cellular account numbers.

If you look up at the top there, we have got it—the top line underneath, where it says "status, auto read"—RCC is just the channel that we are using right now. That is the strongest channel that all the cell phones in this area are using. Below that where you see the record number, that means since we have had this set up for an hour, 86 cellular phones have been intercepted by this equipment and I have enough information about those cellular telephones, from their phone number and their electronic serial number, to clone that into another cellular telephone.

Once I have this information—Mr. Stenger had mentioned that we worked one case down in south Florida where calls were being made to the Middle East using stolen account numbers from the New York area. On the bottom display there, those are actually account numbers that were seized from the search warrant location. Someone using a scanner just like this in the New York area would capture all this information onto a disk and we found that every day they federal expressed that disk into West Palm Beach so that the cloning activity in the operations in the Middle East could continue. And this is just this list here that shows number after number, 26,000 in all, that were used to facilitate that operation.

The highlighted information there indicates that the pin numbers from those phones were captured as well. Sometimes as fast as the industry is able to put in security measures such as personal identification numbers to secure their system, the bad guys develop a new way to come on board and steal that information as well.

Once they have stolen the information—and I will use a phone number that we have captured this morning—we use equipment like this copycat box that is as small as this and can be carried around and it is very portable. We will seize these out of vehicles, out of search warrant locations from a variety of types of cases, not only just a full cloning operation but, in working in cooperation with other agencies, we seized them from drug operations, weapons dealing locations, and search warrants with a variety of crimes.

By hooking this box up to another cellular telephone—these phones are typically stolen phones. We find that a lot of times—for example, in the Miami area, there was an organized group that would actually facilitate "smash and grab" type robberies; they are called that because usually the window is smashed out and anything that is readily available for somebody on the front seat of a car for example is taken. Phones are a pretty popular target in those types of crimes.

I just took this phone up to my cloning box, the menu comes right up and tells me, okay, enter the new electronic serial number that should go into this phone, and I would use one like the one that just came up on the screen there. You can see the ESN—the E575C86F; that is the internal identity of this phone—of one that was captured right here in this room. One of my colleagues here is actually using that phone. We have controlled that a little bit to make sure we are stealing only our own account number this morning for this demonstration.

So I would clone in right from the menu here V575C86F, hit the enter key on this, and it is actually transmitting that number right into this telephone. Now that I have cloned it, it actually has the exact same identity and is working exactly like the phone that is also legitimately working in this room. I will take this now—and you can actually make a phone call with this, Mr. Chairman.

Mr. MCCOLLUM. I do not have to enter an area code, just dial the number?

Ms. RILEY. Yes, sir.

(Dialing phone.)

Mr. MCCOLLUM. Let us see who we get here. There is some pretty bad static on the line. It is not performing very well. Here we go. Now we are getting through. We are ringing somebody's phone back there I can tell.

Yes, Bill McCollum here. Well, thank you, Mike. I am glad to know the cloning works here. Actually I am not glad to know it, but it is a very good demonstration. Thank you, sir. I appreciate that.

That is very impressive.

Ms. RILEY. Mr. Chairman, this equipment is readily available. The box that I showed you that I actually used to clone that phone this morning runs about $1,000 on the street, and the equipment that was shown you this morning that captures the information can be either the scanner, serial number reader such as this, this small, that you use to enter a roadway in close proximity to other people that might drive by and use their phone in the vicinity of this. It can also be the skies as it was—someone took the internal circuitry from that serial number reader and disguised it into an organizer like this to help thwart law enforcement's efforts in read-

ily identifying something of this nature. That is just an example of some of the types of equipment that we are readily seizing on the street now in connection with all of the cloning activity.

Thank you very much for your time. I have all this here and if you want to see it again at another time it can be——

Mr. MCCOLLUM. I appreciate the demonstration. I think it is a very valuable piece of information that you have given us and I think it is very important that we have the ability to know what these boxes look like, Agent Riley. I gather they come in different shapes and sizes—they are not all standard, if you will.

Ms. RILEY. Yes.

Mr. MCCOLLUM. I am going to ask some questions of the panel, if I could. That demonstration was excellent; it shows us just how easy it is to clone these phones. As I understand it, two numbers are being intercepted by this equipment; is that right?

Mr. STENGER. That is correct. It is the ESN/MIN number that is being intercepted.

Mr. MCCOLLUM. Am I correct that a cell-phone continually sends out some kind of an emission when it is on? So, if I am driving down the road between here and New York City, there could be all kinds of people along the way who could pick up this signal, even though I am not talking on the phone; is that right?

Mr. STENGER. That is correct. It is continually registering on a regular basis for the cell site.

Mr. MCCOLLUM. So somebody can steal this phone's identifying numbers and clone it any time the phone is on—I do not have to be sending a telephone call. Is that right?

Mr. STENGER. That is correct.

Mr. MCCOLLUM. Essentially what does it take—what equipment does it take to clone cellular phones? Agent Riley showed us some different pieces of equipment. What do you call these devices?

Mr. STENGER. I will let her answer that specifically as to what they——

Mr. MCCOLLUM. Do you want to sit down with us, Agent Riley, so that you can explain this equipment and respond to any questions? What do you call these things?

Ms. RILEY. I am sorry, I was getting another question——

Mr. MCCOLLUM. What do you call the boxes that you were showing us? If you had to describe it verbally, what kind of equipment does somebody have to have to clone a phone?

Ms. RILEY. Legitimately, sir?

Mr. MCCOLLUM. Legitimately or illegitimately.

Ms. RILEY. Legitimately, no, there is no reason to change the electronic serial number within the phone. That should stay with the phone for the life of the phone, and the FCC actually mandates that the manufacturers of those telephones manufacture them in such a way that that identity cannot be changed.

Mr. MCCOLLUM. All right. But what does it take for the criminal, the drug dealer, or whoever to clone the phone? It just takes one piece of equipment or what? Two pieces?

Ms. RILEY. That is exactly right. That one piece of equipment that I used, the small black box——

Mr. MCCOLLUM. Right.

Ms. RILEY [continuing]. It is called on the street a "copycat box," or a "modem box." We just call it a black box. That one piece of equipment will allow you to change the serial number in the phone. The other boxes that I had there were actually to steal the numbers in the first place.

Mr. MCCOLLUM. How long does it take? It looked to me like that process was pretty quick—what you just did.

Ms. RILEY. Yes, sir, and I actually did do it there. That is all the longer it takes, no more than 30 seconds to change the identity in the phone.

Mr. MCCOLLUM. How close in proximity does the criminal have to be in order to intercept the information necessary to clone a cellular phone?

Ms. RILEY. Depending on the type of box that is used, the one that is similar to the one you have up there right now, you need to be in pretty close proximity; a matter, let us say, 50 to 100 feet. If I were using that scanner, you can capture any cellular traffic in the vicinity of the cell site that I have got it tuned to, so that could be a matter of miles and gives you considerably greater range.

Mr. MCCOLLUM. So some drug dealer could sit under the Brooklyn Bridge intercepting all kinds of phone numbers to clone; is that right?

Ms. RILEY. Absolutely.

Mr. MCCOLLUM. And he could get them when they are passing over on the bridge or going by somewhere down on another side street or wherever as long as it is within a reasonably close distance?

Ms. RILEY. Yes, sir. Any traffic that is feeding into the cell site that I have got the scanner tuned to would actually work, so it can be a pretty broad range.

Mr. MCCOLLUM. Can more than one telephone be cloned from a legitimate phone? In other words, can you clone a number of phones from one?

Ms. RILEY. Yes, sir, that is a process called "stacking." That is what they usually call it on the street, and what they normally will do is clone numerous telephones to one cellular account. In fact, that is a new marketing tool that the cloners will use; in that, if you want a phone that has only been cloned one time—so you get more access to the service that way, you actually have to pay more for your cloned phone not to have it stacked. But you could put—there is an unlimited number of phones that can be cloned under one account and it just makes the fraud multiply that much faster.

Mr. MCCOLLUM. Can several cloned phones be used at the same time? In other words, if we reproduce this phone 14 times, could you have two or three of them in use at one time?

Ms. RILEY. They cannot use the same switch at the same time. What they will typically do is use them in different cities or you wait your turn. So normally what will happen, if I have more than one phone trying to use the switch at the same time, someone will get through and then all the subsequent attempts will get that fast busy signal——

Mr. MCCOLLUM. Right.

Ms. RILEY [continuing]. But if I am using the phone in different parts of the country or even in different switches in the same vicinity, as many phones as one wants to can use the overall system if they want to.

Mr. MCCOLLUM. What happens if a person dials the number of a cloned phone? Does the legitimate phone ring as well as the cloned phone or just the cloned phone?

Ms. RILEY. The first one that the system sees is the one that will ring. There is no way to control whose phone will actually ring. So if you have been cloned sometimes you will get your phone calls and other times that cloned phone will receive them.

Mr. MCCOLLUM. Now, is there any legitimate use, Mr. Stenger, for the equipment used to clone cellular telephones other than by cellular telephone industry employees?

Mr. STENGER. Not at all.

Mr. MCCOLLUM. Why is it difficult to prove that a person found in possession of this type of equipment has the intent to clone a cellular phone, Mr. Stenger?

Mr. STENGER. The problem we have had is that they have used that as a way to get out of it just as it was brought forth about the slot machines; that there was no intent to defraud, they just had it. They were not using it to defraud or anything. But what we have determined is that these programmed materials have no legitimate use other than to clone a phone and they use disclaimers and try and hide the fact basically by saying, "Just do not say you are using it to clone a phone then it is okay," so we need to address that more.

Mr. MCCOLLUM. Mr. Bocchichio and Mr. Navarrete, I assume that you would concur that we need to do something about this. You have both suggested various things. Some of what has been suggested is to have a requirement in law that it is illegal to simply possess some of this equipment that Agent Riley showed us this morning unless you are a legitimate manufacturer, law enforcement agency—somebody who has a defined legitimate reason to have this type of equipment.

Do you favor that type of law? Would it be effective. Would it assist you, as opposed to having to prove the fraudulent intent that you have to prove now, if you could have a separate crime for somebody just simply possessing this equipment? Mr. Bocchichio.

Mr. BOCCHICHIO. It definitely would. It would make it much easier for us. Right now the way the system is, we have to get another Title III and go through the process to intercept a cloned phone; we have to go through the full process of Title III because of the way the law is written today. But here you have an illegal phone, you do not have the consent of anyone to use it, it is totally illegal, and they are committing a crime just by the fact of using it so I do not think the same standard should exist.

Mr. MCCOLLUM. Mr. Navarrete, what do you think about a simple possession type of crime for this equipment for somebody who is not a manufacturer or a cellular company or whatever?

Mr. NAVARRETE. Well, I concur with my colleague and I would like to maybe put—because of the advances in technology, I would like to put the onus maybe on the manufacturers because they are the ones that I think ultimately control it and I think that the

technology is there today that we can make these new phones where they could not be cloned.

Mr. MCCOLLUM. Right. What you are saying is that you believe the phones themselves could be manufactured in a way that they could not be cloned. Does the FBI, Secret Service, of DEA have any scientific studies that would provide a basis for that assertion?

Mr. NAVARRETE. Yes. We have those studies and, if you like, I can get the information to you.

Mr. MCCOLLUM. It would be good information for the record because I would like to know what the technical problems are. Right now, I do not know how costly or easy it would be for the industry to change its manufacturing habits—but it would certainly be intriguing to see about that problem. How extensive is the problem among individuals who are not engaged in some other criminal activity like drug trafficking or involvement with gangs and so forth—just ordinary people who buy this equipment and clone phones to save money?

Mr. NAVARRETE. That is a problem and that is where we work with the industry a lot to really define those groups that are causing the most egregious problem and committing the most fraud. But because they can obtain this equipment so readily, through mail order or how ever, you can have the individual just go out and do it themselves. But what we found more and more being the case, as the problem spreads out into some of the smaller markets, moving from some of the urban areas where security enhancement has been placed, is that groups are still going forward with this and it is actually a business which is producing a large dollar amount of money from the criminal activity.

Mr. MCCOLLUM. I could continue asking questions, but we have been joined by a couple of my colleagues. I certainly know that they are fascinated by the equipment. I can see one of them examining it over there right now. I think I should yield 5 minutes to Mr. Hutchinson if he has questions. Mr. Hutchinson.

Mr. HUTCHINSON. Thank you, Mr. Chairman. I apologize to the witnesses for coming in late. There was another markup where I had to cast some votes but I was briefed earlier in the week on this issue and I know how important it is to the communications industry, as well as to law enforcement, and it is an issue that is very much of a concern.

Mr. Navarrete, your testimony, in answer to the Chairman's question about how industry should address this and make telephones more difficult to clone. But the question I think—and I was not sure of your answer—but do you believe that we should make simple possession of the box that can decode this a crime?

Mr. NAVARRETE. Yes.

Mr. HUTCHINSON. All right. So even though you believe industry should address it, it is important to make it a criminal offense for simple possession without proving intent?

Mr. NAVARRETE. Yes, because, you know, as it has been pointed out, you know, what other legitimate use is there for this type of equipment?

Mr. HUTCHINSON. Well, I notice that this equipment was manufactured in the United States of America. It had in very proud labels, "Made in the USA." I mean the industry that manufacturers

this, would they stand in here and argue that there is some legitimate purpose for this or what is the market they are manufacturing it for?

Mr. NAVARRETE. Well, I am sure they will. They will argue that. That is where we have to have a meeting of the minds, I think, with law enforcement and the industry.

Mr. HUTCHINSON. I guess I am asking you to play devil's advocate a little bit. Would they indicate that there is a legitimate market for this?

Mr. NAVARRETE. I do not know. I am not prepared to speak on that.

Mr. HUTCHINSON. Now, you indicated that simple possession should be a crime. Are you aware of any other simple possession crime without the requirement of intent that exists in the Statutes? I can think of drug paraphernalia and I am not sure that is a good comparison, but are you aware of any comparable statute that exists?

Mr. STENGER. Counterfeit money, simple possession is enough.

Mr. HUTCHINSON. That would be a sufficient comparison. I think there are others that we have not made intent a specific requisite for it. How prevalent is this on drug dealers in the use of the drug trade?

Mr. BOCCHICHIO. It is quite prevalent. The traffickers that deal from Colombia and Mexico into the United States now have gone to other methods than cloned phones. But the surrogates that deal in the United States are—especially the Dominican gangs, the African American gangs and that type of gang—are using cloned phones. The Colombian organized crime gangs, cartels have gone to more sophisticated equipment and as things change, they will do that. As we get better at doing what we do, they get better at doing what they do. They have the money to spend and they will go to higher technology.

Mr. HUTCHINSON. Well, if we have a technological response to this, do you know whether there would still be a technological way to evade that or do you know the direction they are going?

Mr. BOCCHICHIO. You could use basic fraud to evade it by getting a false ID and going into a cellular store and buying a phone using a false identification, and then you could run up a bill on that until it stops. People are doing that too, so that is just basic fraud. We run into that too.

Mr. HUTCHINSON. Do you know of any other nation in which it is illegal for simple possession of this device?

Mr. BOCCHICHIO. Not off the top—no, I do not know.

Mr. HUTCHINSON. Okay. Thank you, Mr. Chairman, I yield back to balance by time.

Mr. MCCOLLUM. Thank you, Mr. Hutchinson. I am going to yield to Mr. Chabot but it reminds me of a follow up question that really ought to be asked here. Do you gentlemen in law enforcement believe we should make it a crime as well for the manufacturer or the retail or wholesale distributor to sell these boxes to anyone other than a specified legal entity who legitimately should have this equipment? Do you think we ought to make it a crime to actually sell to other people?

Mr. BOCCHICHIO. Yes.

Mr. MCCOLLUM. In addition to possession?

Mr. BOCCHICHIO. Yes.

Mr. MCCOLLUM. And you would agree Mr. Navarrete?

Mr. NAVARRETE. I would agree with the caveat that, as you know we have other countries that are excellent at copying our technology and for example, you know, we are focusing the problem on this country but in many instances with the major drug cartels—it is not uncommon to find that they have superior equipment than law enforcement and sometimes that equipment, it is not necessarily U.S. made. It comes from other parts of the world.

Mr. MCCOLLUM. So, you are saying that you would not have that as the exclusive remedy? The possession and the change of the cellular phones would be the more effective method of doing this.

Mr. NAVARRETE. That is correct.

Mr. MCCOLLUM. And you would agree, Mr. Stenger?

Mr. STENGER. Yes, correct. And also I would like to answer, the United Kingdom makes it a law to simply—it is a violation to simply possess it. And I think that brings out one of the areas that needs to be address in conjunction with this is that this is a global problem, it is not just the United States. But many of the nations overseas look to us as being the forerunner in putting forth legislation; Mexico, as we speak, we are putting a presentation on and this is one of the areas they are talking about, the problem with the cloning of phones. So they look to the initiation and enhancement of our laws as kind of a basis for theirs also.

Mr. MCCOLLUM. Mr. Chabot, you are recognized for 5 minutes.

Mr. CHABOT. Thank you, Mr. Chairman, I will be relatively brief. A staffer just gave me a presentation here on how this all works and as always happens around here, we have several committees going on at the same time so I apologize for getting here a little late. One question that comes to mind and this may have already been asked, but is there—do you have an estimate of the percentage of calls that are made out there that are bogus that have—that are illegal, that have been stolen and used off of one of these devices or whatever? Is there any idea of what percentage we might be talking about?

Mr. STENGER. We would not have that. The industry would probably be the ones to really have, at least, a close approximation of how much because they are the ultimate victims. What we have seen is the divergence of the problem to the smaller markets from the urban markets. But the smaller areas where some fixes have been in place in the larger markets so, therefore,—just like, you know, in a bank, if you institute security features like a finger print, they will go across the street to the bank that does not have it. So that is where we are seeing more activity spreading out.

Mr. CHABOT. Okay. And also—and I know we will be considering legislation here—but do you have any recommendations for the public until action is taken to hopefully remedy this situation? Do you have any recommendations? I guess people, obviously, should check their phone bills but what happens sometimes—I would assume many companies have a lot of people using the phones and may not even be aware until they are fairly far down the line as to whether they are paying for calls that somebody else has made. Would you like to comment on that as to basically what you would

recommend the public do to protect themselves until we take some action which might help?

Mr. STENGER. I think you brought out a good point; check their bills. If they see a lot of calls that they are aware of or if they are getting phone calls from people that they do not know—if their phone is ringing and if they are calling out, and they cannot get on the system because they are being blocked because some of the other people are using it.

I think another important thing for the public to realize is this is a crime. Owning and having in your possession a cloned phone and using it is a crime. Sometimes we run into people that looked at it as being, "Well, it is not really a crime." It is, in fact, a crime. The money that is generated from that to the criminal element is used for a lot of other activities and they have to be made aware of that.

Mr. CHABOT. Thank you very much and I thank the Chair. I yield back to balance my time.

Mr. MCCOLLUM. Thank you, Mr. Chabot. Going back to the Cellphone ESN reader—I want to make sure I understand this—you are saying that there is no legitimate use for this unit in the industry in terms of checking phone signals by technicians and so forth? This is manufactured purely for illegal or illegitimate purposes?

Mr. STENGER. That is not one of the items that we were talking about. We were talking about the programming equipment to actually—once the ESN/MIN is seized by that, then it is inputted into a phone; that is the equipment we are talking about. The programming equipment itself.

Mr. MCCOLLUM. Okay. But there is a legitimate use for this unit?

Mr. STENGER. There is, for the industry uses it for technological checking of the phone and things like that.

Mr. BARR. [presiding] Okay. Then tell me again, please, if you would just clarify—while we were talking, a couple of the members were talking a few minutes ago about whether or not we should make simple possession of certain equipment illegal. What is that equipment that we are talking about?

Mr. STENGER. That is like that equipment over there. The modem box, things like that. The actual programming equipment. Once the ESN/MIN is seized——

Mr. BARR. That is this?

Mr. STENGER. That would be that where they actually used that to input into the phone and clone the phone; that is the material we are talking about. And that is the stuff that is advertised in many newspapers and periodicals of offering to sell it to you.

Mr. BARR. On the bottom of this one, it says Motorola and then a number. Would that—does that mean that Motorola made this?

Ms. RILEY. No, sir. That just references that Motorola phones can be cloned using that box and then the numbers that come after it are the passwords for that particular unit. It is password protected so there is just a sticker on the bottom so that, as we try to get that to activate, we use those passwords to make it work.

Mr. BARR. Okay. One thing that comes to mind when we talk about making simple possession of a unit is radar detectors. A radar detector—I cannot think of really any legitimate purpose for

a radar detector other than to detect radar and avoid getting a ticket for speeding. Other than I guess Virginia and maybe one or two other states, simple possession of a radar detector is not illegal because mere possession of it is not commission of a criminal activity. I just would have some concern saying simply because a person with some technical capability has in their possession—or maybe they do not have the technical capability if they are just the recipient of it—the simple possession is illegal. And frankly I think that might be sort of a simplistic approach to solving this. I would be interested, when we have our next panel, to hear from industry what steps industry could take as Mr. Navarrete was saying earlier.

With all of the work that you all are doing, do you really want an additional mandate and an additional burden that now you are going to go out and try and arrest people that have, you know, some sort of technical equipment just by mere possession of it. Where is it not really the use of it for criminal purposes that is our concern?

Mr. STENGER. Yes, I think that is the concern because once they get the cloned phone, the cause problems for law enforcement, for tracing them, tracking them. They conduct business in a relative sphere of anonymity. It causes a—they sell it. They open up businesses with these cloned phones. So it is just—it is what generates the problem after the phone is cloned and that is what we are trying to address here because we have seen too many activities where we are not able to prosecute them in a proactive sense rather than a reactive. I think law enforcement sometimes becomes to reactive to a problem that is already out there.

So being proactive and trying to address the problem that exists and trying to come up with a technical answer to it, in a situation where it is basically free for them to sell these things with a disclaimer, is what we are trying to do here. Maybe Mary can address that.

Ms. RILEY. Our intention is to help stop the manufacture and distribution of this equipment so that the end users do not have such free access to obtain that equipment that we are referencing today. Stopping the advertising, being able to go after the shops that just freely market this to anyone who wants to purchase it. Many of them are the people that are under investigation by the other agencies that are represented here today. It is those groups that we are trying to use some enforcement through this legislation to be able to stop their activity in the manufacture and distribution.

Mr. BARR. What is being done though currently, for example, at the local level? I would presume that most, if not all states, have laws that would encompass with any existing laws the use of this equipment to steal phone numbers. It would be various fraud and threat statutes. A couple of years ago I had a mobile phone stolen out of my car exactly under the circumstances that you indicated; somebody busts the window, takes whatever is readily available and that included a cell-phone and then cloned it. At the time I was speaking with somebody from the phone industry about a replacement phone and they said that you can travel around freeways and you see characters using this equipment standing on the

overpasses getting the numbers as the cars go underneath. The thought came to my mind, why does somebody not arrest them?

Is there really enough, rather than searching out for some new and I think somewhat simplistic new law, is it you all's impression that enough is being done currently in conjunction with local and state officials to really go out and arrest and prosecute these cases now?

Mr. STENGER. We work in a task force environment, whether it is federal or local or state police, and all those laws are applicable to the task force and if we cannot get them on a federal violation and there is an applicable state violation, we will work with the state authorities on that. The problem we are seeing more and more is the fact that it is interstate and international and that is really the federal Lexis here and what we should be addressing.

They can clone phones in Mexico. They can clone phones in the United States with using this equipment and they can traverse the border with global roaming agreements. So we do work with the local prosecutors and address the problem. We have seen this as a problem area that we felt needed to be addressed with an enhancement to this and that is what we are trying to accomplish here because of the fact that they may be applicable in New York, but if they go over to New Jersey there may be an old applicable law.

Mr. BARR. No, and I agree with you and I think that we ought to be looking to see whether or not, particularly our federal laws which regulate people's activities when it becomes illegal and it becomes fraudulent and so forth. If our current laws are not modern enough, strict enough, technically sufficient to attack this problem both domestically and especially internationally, I would be very interested to see if Mexico, whom you mentioned earlier, is a little more forthcoming assisting us in this area than they have been in assisting us in other aspects of the drug enforcement area, particular the problems that they give DEA, so I would be interested in a progress report later on to see if they are really serious about that or whether it is just, you know, words.

But what I am concerned about is if we sort of get off on this tangent of, "Hey, let us make just the mere possession of the equipment illegal," that that is going to solve the problem. I think that we really need—because particularly internationally that is not going to really solve the problem.

You need, I would think, to look at certain perhaps types of international protocols, treaties, and so forth, as well as—as I said, I would be very amenable to looking at any changes that might be necessary that you all could propose to our existing federal statutes that would really strengthen our ability to go after these people performing these acts; not just mere possession of the equipment. I just do not think that that is really going to solve the problem. Any other comments? Mr. Hutchinson, did you have any other questions for this panel?

Mr. HUTCHINSON. I thank the chair. I did want to follow up with one area of inquiry with the DEA or Secret Service. In presenting these cases to the prosecutors, you mentioned that you had one problem with the difficulty of the intent part of it and I assume that there would be a reluctance on their part to pursue some cases

because of difficulty of proving intent. Has there been any other resistance by prosecutors in pursuing these type of cloning cases or possession of these devices?

Mr. STENGER. No, because of the nexus of the cloning you have the cloning operations that are generating money so they address those. And they also realize how it is tied into other criminal activity in providing money so we have been—I think we have had a pretty good reception from the prosecutors on these things.

And I think that if we come to them and we are dealing with the industry and the industry comes forward and says that there is a new technical problem out there, that they are able to get into the system, and overcome some systems security that they put in and then somebody overcomes it, and they come to us with this problem and they say it is going to cause, you know, a tremendous amount of loss and fraud and that the money is going to go somewhere else, we have found that the Justice Department is pretty amenable to the prosecution really.

Mr. HUTCHINSON. And so it is primarily a difficulty of the intent portion of the statute more than a willingness of the prosecutors to pursue these cases; is that fair?

Mr. BOCCHICHIO. I would say that.

Mr. HUTCHINSON. And I think these discussions are good. You raised a question concerning radar devices. Can you think of any—I can not think of any legitimate use for these radar devices or the cloning devices. Perhaps the next panel can enlighten us on that so I will pass the microphone back.

Mr. BARR. Thank you, gentlemen. Did the gentleman from Ohio have any further questions?

In that case, I want to thank you all very much for being with us today, both for the technical expertise you bring in the demonstrations as well as the vast knowledge that you bring to bear and it will help us tremendously in our work in this area and we thank you all very much.

We are happy now to welcome our next panel to focus on the industry side of the equation here, and while our panelists are being seated and getting comfortable, I would like to introduce them to the audience and to the members here.

Mr. Thomas Wheeler is President and CEO of the Cellular Telecommunications Industry Association. He has been involved in telecommunications policy and technology for 20 years and has founded or helped start multiple companies offering cable, wireless, and video communication services, both domestically and internationally. He served as President of the National Cable Television Association from 1979 to 1984. He is also a member of the Board of Trustees at the Kennedy Center for the Performing Arts, the Vincent T. Lombardi Foundation, and the United States Capital Historical Society. Mr. Wheeler is a graduate of the Ohio State University. Mr. Wheeler, we welcome you here today and appreciate your time and effort.

To his left is Mr. John Marinho, who is the Technology Director of Lucent Technologies. He is responsible for the standards, development, and industry relations organization at Lucent. His background is in the areas of mobile and personal telecommunications, circuit and packet switching systems, radio tracking systems, and

network signaling systems. The group he heads at Lucent deals with domestic and international wireless and personal communications standards, coordination, and federal regulatory matters. He received his bachelors degree in electrical engineering from the New Jersey Institute of Technology and holds a masters degree in business administration from Rutgers. He appears today on behalf of the Telecommunications Industry Association. Mr. Marinho, thank you and welcome.

If we would now, Mr. Wheeler, if you have some opening remarks if you would, please, limit them to 5 minutes. Your entire remarks and any additional material that you would like to submit will be printed in their entirety in the record. And then after you make your remarks Mr. Marinho will, and then we will have questions from the panel. Mr. Wheeler.

STATEMENT OF THOMAS E. WHEELER, PRESIDENT AND CEO, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Mr. WHEELER. We appreciate the attention that the subcommittee is paying to this issue today, and before I start my testimony I would be very remiss if I did not salute the people who were sitting in these chairs previously for the job they have been doing, especially the Secret Service. Despite the shortcomings in the current law, they have been effectively trying to do their job and that should not go unheralded.

What you heard in the first panel was that law enforcement officials say that the cloned phone is the crooks' communications device of choice and basically that is because it allows a crook to become an electronic invisible man and to hide behind the identification of a legitimate subscriber like you or me. You have been cloned, I have been cloned; they have hidden behind you and me.

The demo that Agent Riley gave was a terrific demonstration of how the criminal grabs the signal out of the air, programs it into the phone, and thus becomes electronically invisible; takes on the persona to the network of a law abiding citizen like you or me. The law says that this is an illegal act. Unfortunately, the law also says that there must be an intent to defraud.

Now, Mr. Chairman, going to some of the points you just raised—let us take a look here for a second at how easy it is to get equipment that you were just looking at. This is a magazine called "Nuts & Volts," which is a hobbyists's magazine, the August, '97 issue. These red tabs are all ads for these devices readily available:

Here is a full page ad, "Order yours today," with an 800-number. The thing I find interesting is down here at the bottom it says, "About us; we are participants in the Better Business Bureau's Care Program," and then it goes on and drives this full page ad like a Mack truck through the loophole in the law by saying, "all products are sold only for educational purposes," therefore, there is no intent. This is not the Encyclopedia Britannica. There is no educational purpose in selling this device.

Here is another ad, S&N, the Electronic Superstore. It says, "Please call your courteous service representative for complete details." Please call your courteous service representative so you can have a device with which to commit a crime! And then they take advantage of the loophole in the law and say, in the fine print at

the bottom, "Agreement for purchasing of cellular programming software and equipment: Purchaser agrees not to use said software and equipment for any illegal purposes." Now, we should all sleep better with that!

Here is what you can get off the Internet, reams of material. My favorite is this one headed, "$100 per hour cloning cellular phones." It is a new growth industry! Here is how to commit this crime, right here on the Internet and it is advertised on—you go commit this crime, you can earn $100 an hour committing this illegal act. And the reason they get away with this is because of the issue of intent to defraud.

There is only one reason, other than for law enforcement or the industry itself, to have a device like these—that is to enable the commission of a crime. Collecting electronic identification numbers, which is what this device does, is not the hobbyists's activity. Collecting electronic identification numbers is not collecting stamps. These devices exist for the sole purpose of making crooks electronically invisible for the perpetration of other crimes and for perpetrating an economic crime, and as the previous witnesses have said, that economic crime amounts to hundreds of millions of dollars a year.

Now, the good news is that the carriers stand behind their customers when something like this happens, as I am sure, Mr. Barr, you experienced. Your carrier did not charge you for those fraudulent calls to your phone.

The better news is that we have new technology in place that is shutting down the amateur, if you will, who is involved in cloning activities. But the bad news is that that new technology is not stopping the professional; the cloning lab that exists for the purpose of supplying these illegal phones to people who will use them to commit a crime. And the worst news is that those professional cloning labs have the economic incentive and the technological wherewithal to engage us in a technology arms race.

We have leaped out in front of the bad guys right now in terms of technology to stop cloning. They are going to respond and we are going to be in an arms race. We are prepared for that arms race, but we have to use every tool possible, including going after the electronic crooks with a strong law that says, "We know why you have these, there is only one thing you can do with this and that is commit a crime." And what this bill does is to shut down these kinds of advertisements; this kind of $100 an hour offer. This will shut down the ready supply and will help law enforcement get convictions. So we support this legislation, that is why we join law enforcement in supporting it.

Let me make one final amendatory note about a way that you can tighten this bill even more: In 1994, Congress passed the current law and thought they were doing the job and here this "intent" loophole invalidates those activities. If this bill becomes law, the bad guys are not going to stay static; they are going to look for "new" things to do. What this law does is deal with the hacking of a phone and if that becomes more and more difficult, the bad guys are going to bump off of that and go look, "What is the next thing I can hack," and that is obviously the network.

And so one of the things you might want to consider including in this legislation is the same kind of concept that you already have in Section 1030 of Title 18, the very next section that you are dealing with—from what you are dealing with here—which is to also make it illegal to hack the network and in that way maybe we can have a preemptive strike anticipatory of where the crooks are going to go and not have to be back here yet again saying, "Well, they bounced off the good that you did and went to do something else."

Thank you for your attention to this matter and we urge your rapid approval of this anticrime legislation.

[The prepared statement of Mr. Wheeler follows:]

PREPARED STATEMENT OF THOMAS E. WHEELER, PRESIDENT AND CEO, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION

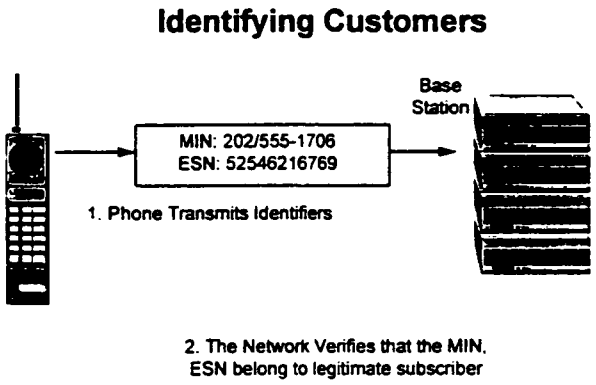
Thank you, Mr. Chairman, and members of the Subcommittee, for the opportunity to present testimony on the wireless industry's war on the criminal cloning of wireless telephones and to discuss the industry's perspective on pending legislation to facilitate law enforcement efforts to conduct criminal investigations and arrests of individuals who steal wireless service through cloning. I am Thomas E. Wheeler, President and CEO of the Cellular Telecommunications Industry Association (CTIA), representing all categories of commercial wireless telecommunications carriers, including cellular and personal communications services (PCS).[1] My testimony today will discuss how the wireless industry has turned the corner in the fight against illegal theft of wireless service by employing an array of high-tech anti-fraud weapons. I will also explain that although the wireless industry has made this type of fraud more difficult, there are and will continue to be criminals with the means and desire to steal wireless service. Finally, I will discuss why law enforcement is current experiencing difficulties in prosecuting these criminals, difficulties that can be addressed with forward-looking anti-cloning legislation.

How Criminals Commit Wireless Fraud

Cellular telecommunications service was initiated for the first time in the United States in 1983. Wireless telephone service has grown faster than any other communications service in history, with over 50 million Americans currently subscribing. The problem of

[1] CTIA is the international organization which represents all elements of the Commercial Mobile Radio Service (CMRS) industry, including cellular, personal communications services, and wireless data. CTIA has over 750 total members including domestic and international carriers, resellers, and manufacturers of wireless telecommunications equipment. CTIA's members provide services in all 734 cellular markets in the United States and personal communications services in all 50 major trading areas, which together cover 95% of the U.S. population.

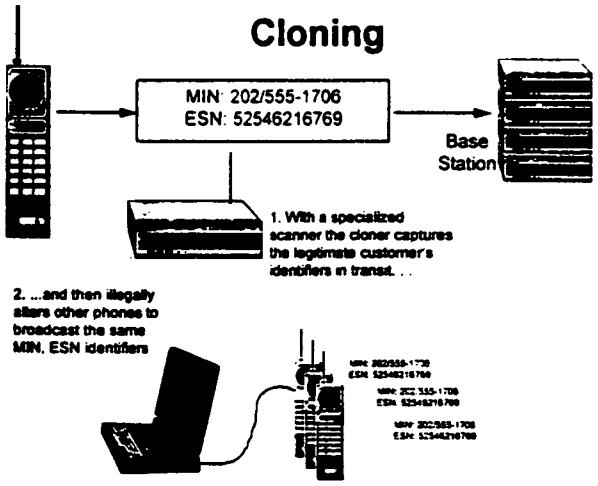
wireless fraud first appeared at a significant level in 1990, when substantial numbers of criminals began using unique electronic scanners to intercept the identifying codes that wireless telephones transmit during their normal operation. Every wireless telephone has a unique pair of identifying numbers which are used to identify phones as they move from cell to cell on a wireless system. One of these numbers is the 10-digit telephone number assigned to a customer by the wireless service provider. In cellular, it's called the Mobile Identification Number or MIN. The other is a 13-digit number that uniquely identifies the phone itself, called the Electronic Serial Number or ESN.



A unique ESN is encoded in every wireless handset by the manufacturer. The relationship between the MIN and the ESN is very much like the relationship between an automobile's license plate and its Vehicle Identification Number or VIN. License plates can be changed as the car is sold or moved to a new state; VINs are permanent numbers

that stay with the vehicle for its life. While a wireless telephone is operating it transmits its ESN/MIN pair periodically in order to tell the system that the phone is on and in which cell it is currently located.

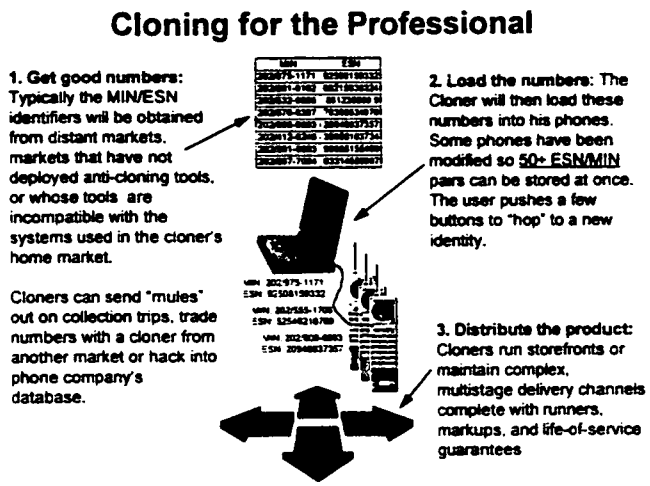
In order to clone a phone the cloner typically employs a unique type of scanner to capture a legitimate ESN/MIN when it is transmitted, and then uses a laptop computer with specialized software to program these numbers into other phones.



To obtain the ESN/MIN numbers the cloner will typically operate an electronic scanning device near a busy highway, tunnel, or airport -- anywhere there is likely to be a high density of traffic transmitting ESN/MIN pairs to the wireless system. Once the scanner has captured an ESN/MIN pair, the cloner reprograms the stolen ESN/MIN pair into other phones so they will mimic the legitimate customer's handset. Programming a

stolen ESN/MIN pair into a wireless telephone using a laptop computer takes only a few minutes.

The cloner typically sells the cloned phone to someone desiring wireless service. The cloned phone then is operational until the wireless carrier discovers the fraud and shuts off that handset's communications capability. Once criminals discovered this cloning technique, they began to seek and obtain both the ESN scanners and the devices used to re-program wireless phones to create the clone. As demand for wireless service increased, criminal cloning matured from an industry of back-room amateurs to more sophisticated professional cloning operations.



The Industry Responds to Cloning

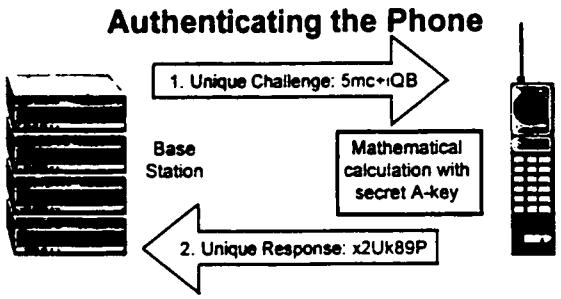
The CTIA and its Board of Directors quickly recognized the potential scope of this problem and created an inter-carrier Fraud Task Force (FTF) in 1990, and soon after established a full-time anti-fraud program at CTIA. In partnership with law enforcement agencies and its members, the wireless industry has rolled out an arsenal of high-tech tools which help defeat the cloner's attempts to steal wireless service. At first, the tools helped industry detect fraudulent use, using technology similar to that used in the credit card industry to detect fraud. Subsequent technologies actually *prevent* cloning, using methods first developed by the military.

While these technologies have proven very successful in stopping consumer-level fraud, they are not a substitute for criminal legislation. History has taught that criminals and the wireless industry are in an "arms race" where new technologies engender new criminal responses. Additionally, there will always be millions of pre-authentication technology phones in usage constituting a bright beacon inviting criminals. Meaningful legislation and effective law enforcement is necessary to close these two cracks in the system.

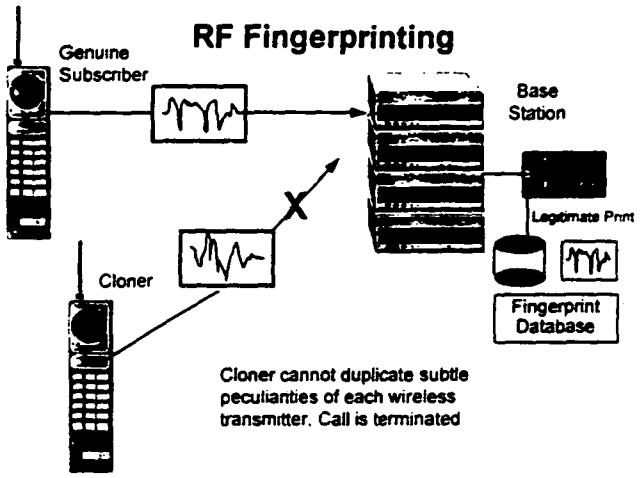
Over the past several years, the wireless industry has developed anti-fraud technologies to authenticate legitimate wireless telephones (Authentication), identify unique wireless telephones via the characteristics of their individual signals, (RF Fingerprinting), verify roaming telephones (Roaming Verification Reinstatement or RVR), identify fraudulent usage at the system level (profiling), and identify legitimate customers (with PIN numbers):

Authentication: Authentication is the latest, and most powerful weapon in the industry's arsenal in the war against cloning. Simply put, Authentication is a system-wide cryptographic challenge/response system that makes it virtually impossible for a criminal to successfully mimic a legitimate customer's phone. The Authentication system has, to date, proven extremely successful reducing industry losses to cloning in markets where it has been deployed.

In order for Authentication to be most effective, all carriers must install the necessary authentication equipment and software. Wireless equipment manufacturers have been overwhelmingly cooperative in producing wireless handsets that support authentication. Although authenticatable wireless telephones have only been available for two years, fully 30% of all wireless telephones in service are either fully authenticatable or capable of supporting authentication. Since virtually all wireless telephones being manufactured now support authentication, the percentage of wireless devices in service that are capable of supporting Authentication will continue to increase rapidly. To complement Authentication, and to verify the identity of wireless telephones that are not able to support this protocol, wireless carriers are deploying additional measures to frustrate cloners. These measures, when used in conjunction with Authentication, will make the use of cloned phones increasingly difficult.

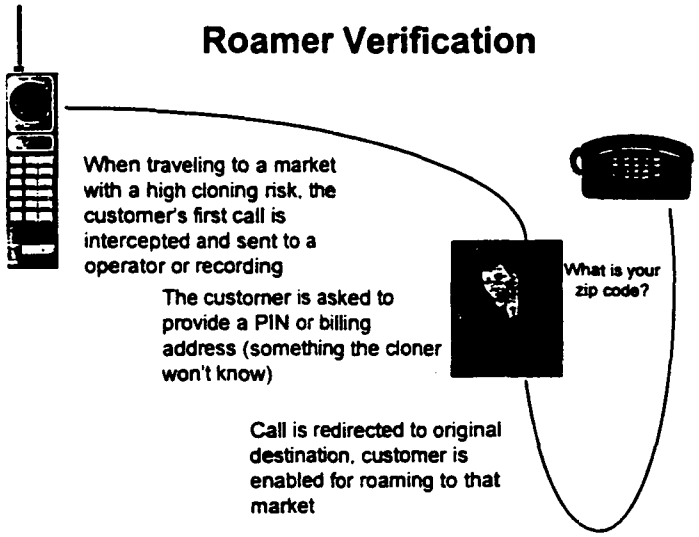


Radio Frequency (RF) Fingerprinting: Some years ago, the U.S. military developed a way to identify, with a high degree of certainty, a particular radio simply by analyzing the unique ways it manipulates radio waves in the course of its normal operation. This identification technology, known as RF Fingerprinting, has been adopted by the wireless industry as a technique for fighting cloning by verifying the identity of individual wireless devices. By comparing the RF Fingerprint of a call to the recorded RF Fingerprint on file for that particular wireless telephone. carrier switches can instantly tell if a phone has been cloned. Carriers in large cities with a high risk of cloning have installed RF Fingerprinting Systems and have dramatically reduced the incidence of cloning fraud, in some cases up to 80%.



- **Roaming Verification and Reinstatement (RVR)**: Cloners frequently use ESN/MIN pairs stolen outside of their home service area in an effort to steal wireless service and remain undetected for a longer period of time. To foil these attempts, the wireless industry now employs RVR to contact wireless customers when a roaming call is made on their telephone to verify that the person using the telephone is the legitimate customer for that telephone. When, for example, a Tulsa customer roams to Miami and places a call, that call will first be routed to a customer service center, which will ask the customer to verify certain identifying information (*e.g.* ZIP code, street address, mother's maiden name).

The legitimate subscriber should have no difficulty in providing this information; the cloner knows nothing about the stolen ESN/MIN combination and will be thwarted.



- **Profiling**: A profiler is a computerized system that charts the typical call patterns of a specific phone. It compares a call with the customer's typical calling pattern. A sudden jump in usage, or two phones being used at once are indicators of a cloned phone. For example, if a subscriber makes a call in New York at 1:00 p.m. on a given day, and then makes a second call from Miami at 1:20 p.m. on the same day, the system can identify that telephone as a likely victim of cloning.

Profiling

The customer's activity is constantly monitored against past usage patterns. Cloning is suspected when:

-There is a sudden jump in the volume of calls

-Calls originate from different cities at the same time

-Calls are made to numbers that frequently appear on bill adjustments (cloners contacts)

Date	Time	From	To
10-May	7:18	Baltimore 14	847/435-7896
10-May	8:51	DOC 5	525-104-4142
10-May	16:33	DOC 6	510/904-3840
10-May	17:05	Laurel 4	301/593-6954
10-May	18:32	Annapolis	301/593-6955
10-May	22:10	Herndon 5	301/587-1984
10-May	23:05	Herndon 7	914/365-7913
11-May	8:12	Baltimore 14	773/399-2630
11-May	10:46	Baltimore 14	202/938-1212
13-May	9:55	Los Angeles	301/593-6954

Profiling allows the early detection of cloned phones, sometimes within minutes, but usually within 24-48 hours of cloning.

- **PIN Numbers**: Personal Identification Numbers, or PINs are used by wireless carriers to prevent cloners from being able to capture all of the data necessary to clone a telephone merely by collecting that telephone's ESN/MIN pair. Working like a PIN on a bank or credit card, a wireless device equipped with a PIN number cannot place a call unless the PIN is entered when a call is placed.

Use of these anti-fraud technologies in concert, coupled with continued and proactive coordination and cooperation with law enforcement at the federal, state, and local level, has enabled the wireless industry to dramatically reverse what were growing industry losses from fraud. We are convinced, however, that criminals will continue to develop new techniques for stealing wireless service, which is why CTIA has developed an

extensive, sustained, and multi-faceted partnership with law enforcement to deter criminals from cloning telephones, and to help catch those who still try.

Coordination With Law Enforcement

In addition to the systematic deployment of anti-fraud technologies, CTIA also established a partnership with law enforcement in order to combat wireless fraud. This partnership includes the following programs:

- **Law Enforcement Training Classes**. Since 1990, CTIA has trained over 15,000 federal, state, and local law enforcement officials in techniques to recognize and combat the crime of wireless fraud. This program is ongoing, with 34 Law Enforcement Training classes scheduled for this fiscal year. The training effort began in the larger metropolitan markets and has now followed the migration of fraud to the smaller and more rural markets. CTIA has retained a full time professional trainer who is a retired United State Secret Service agent to conduct these classes, which focus on showing law enforcement officials the equipment used in cloning, how cloners work, how to develop probable cause and how to effect an arrest.
- **800 Number for Cloning Cases**. CTIA's Fraud Task Force has been operating a nationwide toll-free number for law enforcement officers for the past two years. This number, "1-800-LAWBUST," is currently handling over 3,000 calls per month. This service, operated by CTIA, is available to law enforcement officers 24 hours a day, seven days a week in order to provide timely information relating to cloning. The LAWBUST staff can help police officers display the MIN and ESN from phones they

suspect might be clones, and can also put the police officer in touch with the carrier which issued the legitimate telephone number to determine if fraud has occurred.

- **Private Investigative Firm**. CTIA currently has under contract a private investigative firm that we deploy to assist our carriers in developing wireless fraud cases. These investigators are subject matter experts on wireless fraud.
- **ESN/MIN Losses**: This program is designed to assist law enforcement officers develop the actual and potential losses associated with an ongoing criminal wireless fraud cases. Police officers contact CTIA and provide the ESN/MIN pairs that they have recovered in conjunction with an arrest or search warrant. These numbers are then sorted by carrier and the losses are researched by the individual carrier. These loss reports are then combined and provided to the prosecutor for presentation to the court. This program over the past 20 months has assisted in 87 cases documenting over $14 million in losses. Twelve of these cases have been adjudicated resulting in defendants receiving a total of 30 years in prison and restitution ordered in the amount of $1.5 million.
- **Materials To Assist Law Enforcement in Fighting Wireless Fraud**: Working in coordination with law enforcement, CTIA has developed the following materials and disseminated them widely within the law enforcement community:
    - The Police Officer's Visual Guide to Wireless Fraud Detection
    - CTIA Wireless Fraud Investigations Training Manual
    - CTIA's Wireless Fraud 101 Training Manual
    - CTIA Fraud Workshop and Product Showcase
    - Training and Instructional Videos

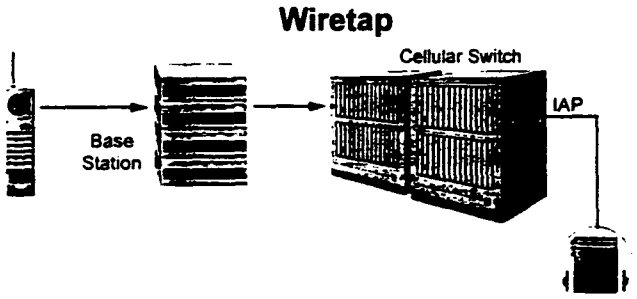
Although our statistics indicate that we have turned the corner on fraud, we know that criminals will seek to find other ways to steal service, which is why we need to sustain our coordination with law enforcement as well as work with the Congress to pass new, forward-looking legislation that will enable law enforcement to successfully prosecute cloners regardless of the technology used. Further, while the industry considers authentication its "nuclear weapon" against fraud, there are still millions of cellular phones in service now that are not equipped for authentication. A substantial number of these wireless telephones will remain in service for years to come, and, as a result, we need to bring the relevant areas of law up to date.

Issues for Law Enforcement

The wireless industry, through the deployment of anti-fraud technologies and constant coordination with law enforcement, has dramatically cut its fraud losses over the past year and expects further dramatic reductions in losses in the months and years to come. While the wireless industry is addressing the consumer side of wireless fraud, the changes in law represented by the draft Wireless Telephone Protection Draft are absolutely necessary for two reasons. First, the proposed changes will further limit the ability of criminals to evade court-ordered wiretaps via the use of cloned phones. Second, the changes help ensure that criminals who clone wireless telephones may be brought to justice.

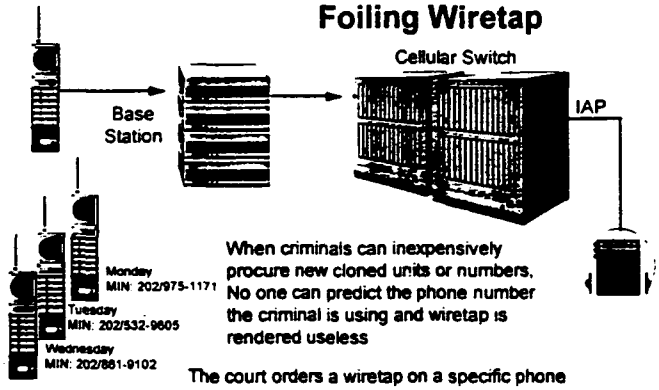
- **Use of Cloned Telephones Helps Criminals to Evade Court-Authorized Wiretaps.** Since the inception of wireless telecommunications in the country just fourteen years ago, wireless carriers have worked side-by-side with law enforcement

in the execution of court-authorized wiretaps to gather evidence, capture, and convict society's most dangerous criminals. In fact, calculated on a per-line basis, a greater proportion of wiretaps are assisted by wireless carriers than traditional wireline telecommunications carriers. We are committed to providing the same support in the years to come. Cloning, however, provides an opportunity for criminals to temporarily evade court-authorized access to a criminal's telephonic conversations. When a law enforcement agency has exhausted other means of gathering evidence or information necessary to bring a dangerous criminal to justice, it will sometimes request from a court the authority to use a wiretap for these purposes. If granted, a court order allows law enforcement to monitor telephone numbers associated with a specific person.



The court orders a wiretap on a specific phone number based on the agent's affidavit. The Switch intercepts and broadcasts a copy of subscriber's conversation to the Intercept Access Point (IAP).

To evade surveillance, a criminal may simply stop using his own home or wireless phone, and instead use one or more cloned phones. That individual will be able to use that cloned phone until the wireless carrier recognizes the use as fraudulent and denies service to that phone. As long as the problem of cloning persists, criminals will have means at their disposal to evade court-authorized wiretaps.



- **Current Difficulties in Prosecuting Cloners.** Current law requires that prosecutors prove "intent to defraud" in order to obtain conviction of cloners under 18 USC 1029. Prosecutors have had difficulty proving intent to defraud when a person is caught with just an ESN reader. For example, in a recent case, United States vs. Yates, a Kentucky man was indicted by a federal grand jury on four counts of criminal fraud following the discovery of his wireless telephone cloning operation by law enforcement officials. In this case, the defendant openly advertised his service to

provide cloned phones to his customers for a price of $150 each. Prior to trial, the defendant's legal team made motions to dismiss his case which the presiding judge denied based on the undisputed facts of the case and the unambiguous legislative history of 18 USC 1029 which specifically criminalizes the defendant's conduct. Nevertheless, in the subsequent trial, the jury acquitted the defendant because, since he did not believe that his service was illegal and, in fact, openly advertised it, he was not operating his service with "intent to defraud" as required for conviction under 18 USC 1029. United States vs. Yates, with news clippings that describe the subsequent jury trial, is Attachment 2. In another case, a district court in California found that using a digital analyzer to detect only the MIN and ESN of a cellular phone did not violate the Electronic Communications Privacy Act.[2]

This difficulty in prosecution, as illustrated in United States vs. Yates, coupled with the relatively light sentences being given for criminal violations, have resulted in prosecutors directing their limited resources to criminals other than cloners.

Congressional Solutions

The wireless telecommunications industry supports the draft Wireless Telephone Protection Act, which was developed in close consultation with the U.S. Secret Service. The proposed legislation makes it a crime merely to possess, prodice, or traffic in hardware or software that has been configured for altering a telecommunications instrument so that it may be used to obtain unauthorized access to telecommunications services. Specifically, the bill:

[2] Matter of Application of U.S., 885 F. Supp. 197, 199 (C.D. Cal. 1995)

- **Removes need to prove intent**. The draft Wireless Telephone Protection Act removes intent to defraud as it pertains to use, production, traffic in, control or custody of or possession of hardware or software that has been configured for altering or modifying a telecommunications instrument so that such instrument may be used to obtain unauthorized access to telecommunications services. This change clarifies the law to show that there is no legitimate purpose for cloning equipment, and would makes possession of these devices a crime. This change would address the Yates problem set forth above.
- **Clarifies legal definition of a scanner to include ESN scanners**. The draft bill also revises the definition of an illegal scanning receiver to make clear that it includes devices that intercept ESNs, MINs or other identifiers of any telecommunications service equipment or instrument. Currently under 1029 an illegal scanning receiver is only defined as a device which intercepts wire or electronic communications in violation of 18 USC section 2510. ESNs and MINs are not considered to be electronic communications and thus are not protected from interception. This law makes illegal a scanning receiver which can receive signaling data even though it cannot receive voice. This is intended to address the Matter of Application of U.S. problem set forth above.
- **Stiffens Penalties for Criminals Who Use Cloned Phones to Perpetrate Other Crimes**. The draft Wireless Protection Act directs the U.S. Sentencing Commission to review and amend the sentencing guidelines to provide appropriate penalties for offenses which involve the cloning of wireless phones.

- **Permits wireless carriers to possess and use cloning devices to fight wireless fraud**. Under current law, telecommunications carriers are allowed to possess and use cloning devices as a part of their ongoing efforts to deter wireless fraud. The draft Wireless Telephone Protection Act assures that this vital capability is maintained. The ability to test or "reverse engineer" such devices as well as scanners and cloned phones will allow telecommunications carriers to continue to develop effective systems to defeat cloning.

Potential Additional Provisions

The draft Wireless Telephone Protection Act focuses on cloning as it is practiced today, where a criminal uses a scanner to capture the ESN/MIN pair of a legitimate phone when it is transmitted and then uses a computer with special software to reprogram other phones with these numbers. Hardware or software that does not alter or modify a telecommunications instrument, but nevertheless can defeat current anti-fraud efforts, could fall outside the provisions of the bill. To address this problem, the bill could be amended to also prohibit the use, production, traffic in, control or possession of a program, information code, or command not provided by the manufacturer of a telecommunications instrument used to originate or terminate commercial mobile radio service. A similar ban is already included in section 1030 of title 18, the computer fraud statue.

Title 18, as amended by the Wireless Telephone Protection Act as currently drafted will continue to require "intent to defraud" for all other crimes except the possession of hardware or sofeware used for altering or modifying telecommunications

instruments to obtain unauthorized access to telecommunications service. This problem could be minimized by making the replication of ESNs or MINs a violation of the counterfeiting and forgery provisions of the U.S. Code, which do not require any showing of intent. Specifically, the provisions of the U.S. Code that currently prohibit counterfeiting and forgery, the importing and exporting of stolen goods, and trafficking in stolen property could be amended to include the counterfeiting or forgery of ESNs; the importation or exportation of stolen subscriber equipment used for commercial mobile radio service; and the trafficking in subscriber equipment used for CMRS where the ESN has been altered.

Summary

The wireless telecommunication industry, through significant investment in anti-fraud technologies and sustained cooperation with law enforcement, has dramatically reduced its losses from cloning fraud. The legislative changes embodied in the Committee's draft Wireless Telephone Protection Act establishes a framework that will enable law enforcement to prosecute those who will still try to commit wireless fraud. We are grateful to Chairman McCollum and this Subcommittee for the ongoing interest in fighting wireless fraud. I would also like to thank the Secret Service for their cooperation and proactive assistance in the field and in developing the legislation that we understand will be introduced later today.

Attachments

1. The Wireless Telephone Protection Act (staff discussion draft dated September 5, 1997).
2. Opinion and Order in Criminal Action No. 95-72, U.S. vs. Don Billy Yates, Jr. and associated newspaper clips.
3. 18 U.S.C. 1025.
4. Examples of Typical ESN Scanners.

ATTACHMENT #1

105TH CONGRESS
1ST SESSION

H. R. _____

IN THE HOUSE OF REPRESENTATIVES

Mr. SAM JOHNSON of Texas (for himself, Mr. MCCOLLUM, and Mr. SCHUMER) introduced the following bill; which was referred to the Committee on _____

A BILL

To amend title 18, United States Code, with respect to scanning receivers and similar devices.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Wireless Telephone Protection Act".

SEC. 2. FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COUNTERFEIT ACCESS DEVICES.

(a) UNLAWFUL ACTS.—Section 1029(a) of title 18, United States Code, is amended—

(1) by redesignating paragraph (9) as paragraph (10); and

(2) by striking paragraph (8) and inserting the following:

"(8) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;

"(9) knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured for altering or modifying a telecommunications instrument so that such instrument may be used to obtain unauthorized access to telecommunications services; or".

(b) PENALTIES.—

(1) GENERALLY.—Section 1029(c) of title 18, United States Code, is amended to read as follows:

"(c) PENALTIES.—The punishment for an offense under subsection (a) of this section is—

"(1) in the case of an offense that does not occur after a conviction for another offense under this section—

"(A) if the offense is under paragraph (1), (2), (3), (6), (7), or (10) of subsection (a), a fine under this title or imprisonment for not more than 10 years, or both; and

"(B) if the offense is under paragraph (4), (5), (8), or (9), of subsection (a), a fine under this title or imprisonment for not more than 15 years, or both; and

"(2) in the case of an offense that occurs after a conviction for another offense under this section, a fine under this title or imprisonment for not more than 20 years, or both.".

(2) ATTEMPTS.—Section 1029(b)(1) of title 18, United States Code, is amended by striking "punished as provided in subsection (c) of this section" and inserting "subject to the same penalties as those prescribed for the offense attempted".

(c) DEFINITIONS.—Section 1029(e) of title 18, United States Code, is amended—

(1) in paragraph (6), by striking "and";

(2) in paragraph (7)—

(A) by striking "The" and inserting "the"; and

(B) by striking the period and inserting "; and"; and

(3) in paragraph (8), by striking the period and inserting "or to intercept an electronic serial number, mobile identification number, or other identifier

of any telecommunications service, equipment, or instrument;".

(d) APPLICABILITY OF NEW SECTION 1029(a)(9).—

(1) IN GENERAL.—Section 1029 of title 18, United States Code, is amended by adding at the end the following:

"(g) It is not a violation of subsection (a)(9) for an officer, employee, or agent of, or a person under contract with, a facilities-based carrier, for the purpose of protecting the property or legal rights of that carrier, to use, produce, have custody or control of, or possess hardware or software configured as described in that subsection (a)(9).".

(2) DEFINITION.—Section 1029(e) of title 18, United States Code is amended—

(A) by striking "and" at the end of paragraph (6);

(B) by striking the period at the end of paragraph (7) and inserting a semicolon; and

(C) by striking the period at the end of paragraph (8) and inserting "; and"; and

(D) by adding at the end the following:

"(9) As used in this subsection, the term 'facilities-based carrier' means an entity that owns communications transmission facilities, is responsible for the operation and

maintenance of those facilities, and holds an operating license issued by the Federal Communications Commission under the authority of title III of the Communications Act of 1934.".

(e) AMENDMENT OF FEDERAL SENTENCING GUIDELINES FOR WIRELESS TELEPHONE CLONING.—

(1) IN GENERAL.—Pursuant to its authority under section 994 of title 28, United States Code, the United States Sentencing Commission shall review and amend the Federal sentencing guidelines and the policy statements of the Commission, if appropriate, to provide an appropriate penalty for offenses involving the cloning of wireless telephones (including offenses involving an attempt or conspiracy to clone a wireless telephone).

(2) FACTORS FOR CONSIDERATION.—In carrying out this subsection, the Commission shall consider, with respect to the offenses described in paragraph (1)—

(A) the range of conduct covered by the offenses;

(B) the existing sentences for the offenses;

(C) the extent to which the value of the loss caused by the offenses (as defined in the Federal sentencing guidelines) is an adequate

measure for establishing penalties under the Federal sentencing guidelines;

(D) the extent to which sentencing enhancements within the Federal sentencing guidelines and the court's authority to sentence above the applicable guideline range are adequate to ensure punishment at or near the maximum penalty for the most egregious conduct covered by the offenses;

(E) the extent to which the Federal sentencing guideline sentences for the offenses have been constrained by statutory maximum penalties;

(G) the extent to which Federal sentencing guidelines for the offenses adequately achieve the purposes of sentencing set forth in section 3553(a)(2) of title 18, United States Code;

(H) the relationship of Federal sentencing guidelines for the offenses to the Federal sentencing guidelines for other offenses of comparable seriousness; and

(I) any other factor that the Commission considers to be appropriate.

ATTACHMENT #2

Eastern District of Kentucky
FILED
DEC 13 1995

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
LEXINGTON

CRIMINAL ACTION NO. 95-71

UNITED STATES OF AMERICA, PLAINTIFF,

V. OPINION AND ORDER

DON BILLY YATES, JR., DEFENDANT.

* * * * * * * * * * * * * * *

This matter is before the Court upon the motion of the defendant, Don Billy Yates, to dismiss. This matter has been fully briefed and is ripe for review.

I. FACTS

Yates was indicted by a federal grand jury on November 2, 1995 on four counts of criminal fraud in violation of various provisions of 18 U.S.C. § 1029. Specifically, count one of the indictment charges that Yates, "knowingly and with intent to defraud, did produce, use and traffic in a counterfeit access device, which conduct affected interstate commerce," in violation of § 1029(a)(1) and (c)(1). Count two of the indictment charges that Yates "knowingly and with intent to defraud, did have control, custody, and possession of device-making equipment, which conduct affected interstate commerce," in violation of § 1029(a)(4) and (c)(1). Count three of the indictment charges that Yates "knowingly and with intent to defraud, did produce, traffic in, have control, custody and possession of a telecommunications instrument that had been modified and altered to obtain unauthorized use of telecommunications services, which conduct affected interstate commerce," in violation of § 1029(a)(5) and (c)(1). Finally, count

four of the indictment charges that Yates "knowingly and with intent to defraud, did use, have control, custody and possession of hardware and software used for altering and modifying telecommunications instruments to obtain unauthorized access to telecommunications services, which conduct affected interstate commerce," in violation of § 1029(a)(6)(B) and (c)(1). Each count alleges that the offense occurred on or about September 18, 1995. At the arraignment on November 9, 1995, Yates plead not guilty to each count.

On November 20, 1995, Yates filed two motions to dismiss the indictment. In his first motion to dismiss, Yates argues that the indictment should be dismissed as multiplicitous, or alternatively, that the United States should elect under which count of the indictment it will proceed at trial. In his second motion to dismiss, Yates argues that the indictment fails to charge him with engaging in an illegal activity. A hearing on the motions was held on December 1, 1995. The Court denied Yates' motion to dismiss the indictment as multiplicitous. However, the Court held that counts 2 and 4 of the indictment are duplicitous and ordered the United States to elect between counts 2 and 4 of the indictment. Yates' motion to dismiss on the grounds that the indictment fails to charge an illegal activity was taken under advisement by the Court.

II. YATES' MOTION TO DISMISS FOR FAILURE TO CHARGE AN ILLEGAL ACTIVITY

The issue in Yates' motion to dismiss is whether a "cloned" cellular telephone -- i.e., one with identification numbers identical to another existing legitimate unit -- falls within the ambit of § 1029. Based on representation from counsel and independent research, this appears to be an issue of first impression.

To determine whether the indictment charges Yates with an illegal activity, an understanding of the cellular telephone industry is imperative. Cellular telephone service is available from commercially owned and operated communications networks and is based upon a system of individual cellular telephone units having wireless radio transmission capabilities and which operate within a series of geographic "cells" served by a radio transmitter. Cellular telephones are typically programmed with two identifying code numbers, commonly referred to as the electronic serial number, "ESN," and the mobile identification number, "MIN." The ESN is a unique numerical code embedded in each cellular telephone by the manufacturer identifying that particular instrument. The MIN is a ten-digit numerical telephone number (area code + seven-digit telephone number) assigned to each cellular telephone customer. For identification purposes, both numbers are transmitted to the cellular system by the cellular telephone unit at the time a call is initiated. As the user moves from one cell to another, transmission of telephone calls is automatically shifted from one transmitter to the other, thus maintaining a consistent signal quality.

Cases construing § 1029 as it applies to the cellular telephone industry have involved "tumbling" cellular telephones. *See United States v. Brady*, 13 F.3d 334 (10th Cir. 1993); *United States v. Bailey*, 41 F.3d 413 (9th Cir.), *cert. denied*, 115 S.Ct. 2563 (1994); *United States v. Ashe*, 47 F.3d 770 (6th Cir. 1995). A "tumbling" cellular telephone is one which is capable of randomly changing either the ESN or MIN to enable the user to obtain a "free ride" through the cellular telephone system by avoiding or defeating access or billing to an individual customer account. Tumbling cellular telephones take advantage of the "roam" feature provided by cellular carriers. Cellular telephone customers may "roam," that is, place calls from a

foreign geographic cell other than the geographic cell owned and operated by the carrier with whom the customer has an account. This allows customers to place a local or long distance call from anywhere in the United States while outside the geographic area serviced by his or her home carrier. When a roamer places a call from a foreign geographical service area, the cellular telephone automatically transmits the caller's assigned ESN and MIN. In processing a roamer call, a foreign carrier immediately recognizes the MIN as belonging to another existing carrier. To provide effective customer service, roamer calls are, by internetwork agreement, practice and procedure, immediately transmitted by a foreign carrier before validation of the identifying ESN and MIN combination has been completed by a central data bank clearing house located in San Angelo, Texas. A time lag occurs while its computers seek to match the automatically transmitted identifying ESN and MIN with an existing home carrier-subscriber combination recorded in its data bank of national internetwork listings. In the absence of a valid match, all subsequent calls using the same ESN and MIN will be rejected. Although service charges resulting from unmatched ESN and MIN combinations are listed together with all pertinent information related to the call in the foreign carrier's billing computer, the illicit roaming customer cannot be identified. As a result, the charges cannot be collected from the user of a tumbling cellular telephone and the cellular carrier absorbs the cost of the call.

In *Brady*, the Tenth Circuit Court of Appeals considered whether tumbling cellular telephones are violative of § 1029. *Brady*, 13 F.3d at 338. The Tenth Circuit relied on *United States v. McNutt*, 908 F.2d 561 (10th Cir. 1990), in which the court held that cloned electronic addresses on satellite television descrambler modules were not "access devices" within the meaning of § 1029. *Id.* at 338-39. Even though the operators of satellite television services

suffered economic losses from the revenue forgone due to the use of cloned descrambler modules, the court determined that there was no violation of § 1029 because use of such modules did not "debit legitimate subscriber's accounts[, and] no additional charges accrued as a result of the unauthorized use." *McNutt*, 908 F.2d at 563-64. In other words, the court in *McNutt* held that "economic losses were not enough under § 1029; instead, the government must be able to connect actual losses to distinct transactions reflected in the company's accounting records." *Brady*, 13 F.3d at 338. Because calls made from a tumbling cellular telephone do not "debit legitimate subscriber's accounts" or "trigger the creation and maintenance of a formal record of credits and debits," the court in *Brady* held that a tumbling cellular telephone is not an access device within the meaning of § 1029. *Id.* at 339.

In addressing the identical issue in *United States v. Ashe*, 47 F.3d 770 (6th Cir. 1995), the Sixth Circuit Court of Appeals rejected the Tenth Circuit's interpretation of § 1029. In *Ashe*, the defendant challenged his conviction under § 1029 for producing and possessing a tumbling cellular telephone. In rejecting *Brady*, the court noted that "[i]n 1992, the losses charged to cellular telephone carriers resulting from 'free riding' amounted to over $100 million." *Id.* at 774. As a result, the court held that "invasion of an identifiable customer's account is not a necessary element of proof to support a conviction under [§ 1029]." *Id.* at 774. Similarly, in *United States v. Bailey*, 41 F.3d 413 (9th Cir. 1994), the Ninth Circuit Court of Appeals held that tumbling cellular telephones are access devices within the ambit of § 1029.

Unlike *Brady*, *Ashe*, and *Bailey*, Yates is charged with use, possession and trafficking of a cloned cellular telephone and cloning equipment. Cloning involves the programming of a cellular telephone so that the ESN and MIN combination is identical to a legitimate customer's

account in order to obtain free telephone service. By obtaining a cloned telephone, a cellular customer avoids an activation fee and a monthly maintenance fee charged by the cellular carrier.

The facts in this case are undisputed. In April 1995, the Secret Service executed a search warrant at a company that was selling or distributing "black boxes" that are used to clone MINs and ESNs. The search yielded a list of customers, including Yates, who had purchased at least one black box. During the same time, the Secret Service also received information from a local cellular telephone company that Yates was using a black box to clone cellular telephones. Basically, Yates' service involved providing customers with an "extension phone" so that they could have two cellular telephones with the same number, while paying the activation charge and maintenance fee for only one cellular telephone. Calls made from either cellular telephone, however, appear on the customer's bill. Yates charged $150 for his cloning service.

On September 18, 1995, Special Agent James Burch of the United States Secret Service obtained two cellular telephones, one of which was programmed with an authorized ESN and MIN, and one which was blank. Burch then contacted and arranged to meet with Yates to obtain a cloned cellular telephone. At their meeting, Yates programmed the ESN and MIN of the legitimate cellular telephone into the blank cellular telephone. Both Yates and Burch made test calls from the cloned cellular telephone. Yates was subsequently arrested and indicted for violating § 1029.

In support of his motion to dismiss, Yates argues that the Federal Communications Commission, the federal agency charged with regulating the telecommunications industry, has consistently held that telephone numbers are not the property of the carrier but are instead a public resource. *See In Re The Matter Of Administration Of North American Numbering Plan,*

... *Of The Need To Promote Competition And Efficient Use Of* ...*trum For* ... *Service*, FCC 86-85 (1986). As a result, Yates contends that the FCC's ruling caused citizens such as himself, to believe that the activity charged in the indictment is not illegal. Yates contends that *United States v. Levin*, 973 F.2d 463 (6th Cir. 1992), is analogous to the present case. In *Levin*, the Sixth Circuit Court of Appeals affirmed the dismissal of an indictment charging an opthamologist with Medicaid fraud for billing practices which the Healthcare Finance Administration had implied were legal. Based on *Levin* and the ruling by the FCC, Yates contends that he cannot be charged with engaging in a fraudulent activity where that fraudulent activity is wholly dependent upon ownership of a cellular telephone number by a telephone carrier.

In further support of his motion to dismiss, Yates argues that because the telephone carrier will continue to be able to bill its customers for all calls made on the extension telephone, they are not damaged by the use of the extension telephone. Moreover, Yates contends that the telephone companies have no right to profit based on the customer's use of a particular telephone number since these numbers are public resources. As a result, Yates contends that the indictment does not charge illegal activity and must be dismissed.

Yates' argument directly contradicts the legislative history of § 1029(a). In 1994, conceivably in response to the Tenth Circuit Court of Appeals' ruling in *Brady*, Congress amended § 1029(a) to specifically criminalize Yates' conduct. In passing the amendment, Congress stated:

> This section amends the counterfeit access device law to criminalize the use of cellular phones that are altered, or "cloned," to allow free riding on the cellular phone system. Specifically, this section prohibits the use of an altered telecommunications instrument, or a scanning receiver, hardware or software, to

> obtain [redacted] access to telecommunications services for the purpose of defrauding the carrier. A scanning receiver is defined as a device used to intercept illegally wire, oral or electronic communications. The penalty for violating this new section is imprisonment for up to fifteen years and a fine of the greater of the $50,000 or twice the value obtained by the offense. House Report H.R. No. 103-8271.

Clearly, Yates' conduct involved the "use of an altered telecommunications instrument . . . to obtain access to telecommunications services for the purpose of defrauding the carrier." Moreover, Yates' argument that the cellular carriers are not damaged by use of the extension telephone is erroneous. By cloning cellular telephones to enable users to have an extension phone, the cellular carriers are defrauded of the activation fee and the monthly service fee they charge for each cellular phone. Therefore, Yates' motion to dismiss will be denied.

III. CONCLUSION

Accordingly, the Court, being sufficiently advised, hereby ORDERS that Yates' motion to dismiss [docket entry 19] is DENIED.

On this 12th day of December, 1995.

KARL S. FORESTER, JUDGE

★ LEXINGTON HERALD LEADER, LEXINGTON, KY. ■ THURSDAY, DECEMBER 14, 1995

Judge won't dismiss charges of cloning cellular phones

BY THOMAS TOLLIVER
HERALD LEADER STAFF WRITER

A Lexington man who argued in court that cloning a cellular phone for $150 was not illegal has lost his bid to get criminal charges against him dismissed.

Don Billy Yates, 36, was indicted Nov. 2 on four counts of criminal fraud, all stemming from possessing and using an electronic device that enabled him to copy the phone number of one cellular telephone onto a second cellular phone.

The copying, or cloning as it is known, allowed Yates' customers to have two phones for the price of one. Although the customer had to pay for any air time generated by the second phone, the customer would not have to pay an activation fee or monthly service fee for the second phone.

Soon after Yates was indicted, his attorney, Burl McCoy, filed a motion to dismiss the indictment because it did not charge Yates with an illegal activity. McCoy argued that federal law did not prohibit what Yates was doing and nobody was being defrauded. But federal prosecutors disagreed.

In an eight-page order issued Tuesday, U.S. District Judge Karl Forester also disagreed.

Forester said Yates' argument that cellular carriers are not damaged by the use of the extension phone is erroneous. By cloning cellular telephones to allow users an extension phone, the carriers are defrauded of the activation fee and the monthly service fee they charge for each cellular phone, Forester said.

Yates is set to stand trial Jan. 2. McCoy, reached yesterday, was still of the opinion that Yates had done nothing illegal.

"We plan to defend the case vigorously, and I have no doubt a jury will find him not guilty," McCoy said.

Jury acquits Fayette man in cellular phone case

BY DARLA CARTER
HERALD-LEADER STAFF WRITER

A Lexington man charged with fraud in the cloning of cellular phones was found not guilty yesterday by a U.S. District Court jur-

on Billy Yates, 36, was acquitted of three counts of criminal fraud for enabling customers to have two cellular phones for the price of one.

The charges stemmed from a federal indictment issued Nov. 2 that accused Yates of the possession or use of an electronic device that allowed him to copy the phone number of one cellular phone onto a second cellular phone.

Though his customers had to pay for any air time generated by the second phone, they didn't have to pay an activation fee or monthly service fee for the second phone.

Likening Yates' activities to copyright infringement and counterfeiting, prosecutor Thomas L. Self argued that Yates was violating the law by cheating phone companies out of those fees.

"He was hurting the industry," said Self, an assistant U.S. attorney.

But Yates' defense team — at-

SEE PHONE, B7

PHONE: Jury acquits man in cellular case

FROM PAGE B1

torneys Burl McCoy and John Kevin West — maintained that Yates' actions weren't illegal. The attorneys also said the prosecution failed to prove a key element of its case: intent.

West pointed out to jurors that Yates widely advertised that he cloned phones for $150 and even offered the service to lawyers.

"He wasn't trying to hide this from anyone," West said. "...'cause he didn't think there was anything wrong with it, and he didn't intend to defraud anyone."

The jury deliberated about four hours before returning not guilty verdicts on all counts.

After the verdicts were read, Yates turned his face toward his family and smiled. And his brother, Dale, raised both fists in a sign of victory.

"It's an undescribable feeling," said Yates.

Nevertheless, ... Yates ... doesn't plan to get back into the cloning business, McCoy said.

Yates is thought to be the first person in the nation to face criminal charges related to the cloning of a cellular phone.

McCoy said the law isn't clear and speculated that Yates' case might spark Congress to do something about that.

Self declined to comment on Yates' acquittal.

But McCoy said, "We're really pleased with the verdict. It again reaffirms my faith in the jury system."

"(a) For purposes of section 1028 of title 18, United States C (this section) to the maximum extent feasible, personal de ptors or identifiers utilized in identification documents, as defined in such section, shall utilize common descriptive terms and formats designed to—

"(1) reduce the recurrency and duplication of identification systems by providing information which can be utilized by the maximum number of authorities, and

"(2) facilitate positive identification of bona fide holders of identification documents.

"(b) The President shall, no later than 3 years after the date of enactment of this Act [Oct. 12, 1984], and after consultation with Federal, State, local, and international issuing authorities, and concerned groups make recommendations (sic) to the Congress for the enactment of comprehensive legislation on Federal identification systems. Such legislation shall—

"(1) give due consideration to protecting the privacy of persons who are the subject of any identification system,

"(2) recommend appropriate civil and criminal sanctions for the misuse or unauthorized disclosure of personal identification information, and

"(3) make recommendations providing for the exchange of personal identification information as authorized by Federal or State law or Executive order of the President or the chief executive officer of any of the several States."

Legislative History

For legislative history and purpose of Pub.L. 97-398, see 1982 U.S. Code Cong. and Adm. News, p. 3518. See, also, Pub.L. 99-646, 1986 U.S. Code Cong. and Adm. News, p. 6139; Pub.L. 101-647, 1990 U.S. Code Cong. and Adm. News, p. 6472; Pub.L. 103-322, 1994 U.S. Code Cong. and A News, p. 1801; Pub.L. 104-294, 1996 U.S. Code Cong. a dm. News, p. 4021.

§ 1029. Fraud and related activity in connection with access devices

(a) Whoever—

(1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;

(2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period;

(3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;

(4) knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;

(5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000;

(6) without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of—

(A) offering an access device; or

(B) selling information regarding or an application to obtain an access device;

(7) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services;

(8) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses—

(A) a scanning receiver; or

(B) hardware or software used for altering or modifying telecommunications instruments to obtain unauthorized access to telecommunications services; or

(9) without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device;

shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

(b)(1) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(2) Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c) of this section, or both.

(c) The punishment for an offense under subsection (a) or (b)(1) of this section is—

(1) a fine under this title or twice the value obtained by the offense, whichever is greater, or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (3), (5), (6), (7), (8), or (9) of this section which does not occur after a conviction for another offense under either such subsection, or an attempt to commit an offense punishable under this paragraph;

(2) a fine under this title or twice the value obtained by the offense, whichever is greater, or imprisonment for not more than fifteen years, or both, in the case of an offense under subsection (a)

(1), (4), (5), (6), (7), or (8) of this section which does not occur after a conviction for another offense under either such subsection, or an attempt to commit an offense punishable under this paragraph; and

(3) a fine under this title or twice the value obtained by the offense, whichever is greater, or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this paragraph.

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section—

(1) the term "access device" means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument);

(2) the term "counterfeit access device" means any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device;

(3) the term "unauthorized access device" means any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud;

(4) the term "produce" includes design, alter, authenticate, duplicate, or assemble;

(5) the term "traffic" means transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of;

(6) the term "device-making equipment" means any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device; and

(7) The term "credit card system member" means a financial institution or other entity that is a member of a credit card system, including an entity, whether affiliated with or identical to the credit card issuer, that is the sole member of a credit card system.

(8) the term "scanning receiver" means a device or apparatus that can be used to intercept a wire or electronic communication in violation of chapter 119.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States, or any activity authorized under chapter 224 of this title. For purposes of this subsection, the term "State" includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.

(Added Pub.L. 98-473, Title II, § 1602(a), Oct. 12, 1984, 98 Stat. 2183, and amended Pub.L. 99-646, § 44(b), Nov. 10, 1986, 100 Stat. 3601; Pub.L. 101-647, Title XII, § 1205(f), Nov. 29, 1990, 104 Stat. 4831; Pub.L. 103-322, Title XIV, § 250007, Title XXXIII, § 330016(1)(D), Sept. 13, 1994, 108 Stat. 2097, 2147; Pub.L. 103-414, Title II, § 208, Oct. 25, 1994, 108 Stat. 4291; Pub.L. 104-294, Title VI, § 601(l), Oct. 11, 1996, 110 Stat. 3501.)

HISTORICAL AND STATUTORY NOTES

Report to Congress

Section 1608 of Pub.L. 98-473, provided that: "The Attorney General shall report to the Congress annually, during the first three years following the date of the enactment of this joint resolution (Oct. 12, 1984), concerning prosecutions under the section of title 18 of the United States Code (this section) added by this chapter."

Legislative History

For legislative history and purpose of Pub.L. 98-473, see 1984 U.S. Code Cong. and Adm. News, p. 3182. See, also, Pub.L. 99-646, 1986 U.S. Code Cong. and Adm. News, p. 6139; Pub.L. 101-647, 1990 U.S. Code Cong. and Adm. News, p. 6472; Pub.L. 103-322, 1994 U.S. Code Cong. and Adm. News, p. 1801; Pub.L. 103-414, 1994 U.S. Code Cong. and Adm. News, p. 3489; Pub.L. 104-294, 1996 U.S. Code Cong. and Adm. News, p. —

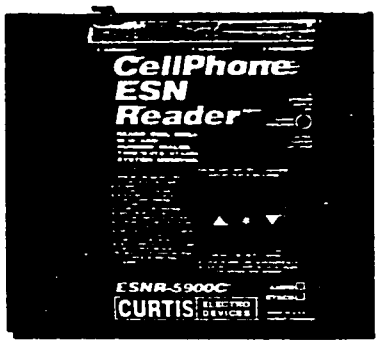
§ 1030. Fraud and related activity in connection with computers

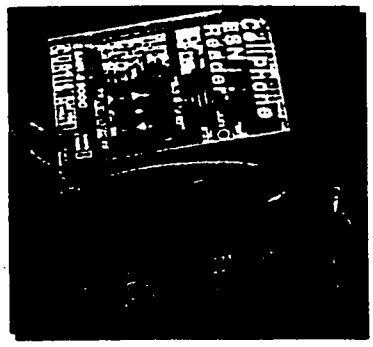
(a) Whoever—

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver,

ATTACHMENT 14

Scanning Devices





SUMMARY

Over the past 14 years, the wireless telecommunications industry has exploded from zero subscribers in 1983 to over 50 million today. As use of wireless service has grown, so too have the efforts of those who would attempt to obtain wireless service through the fraudulent "cloning" of legitimate customer's wireless telephones. In 1990, technology to capture the unique identifying numbers transmitted by wireless telephones and then program those numbers into another phone, thus creating a "clone" of the legitimate phone, began to appear. Reacting to this development, the wireless industry, led by CTIA, immediately began a sustained effort to develop and deploy effective anti-fraud technologies and work with law enforcement to facilitate the arrest of cloners.

To date, the wireless industry has invested millions of dollars to fight fraud, and has deployed a high-tech suite of anti-fraud technologies that:

- deny service to a cloned phone at the start of a call,
- terminate a call if the radio frequency fingerprint of a phone does not match our records; and,
- call a customer for identifying information if a calling pattern shows significant changes.

While these technologies have proven very successful in stopping consumer-level fraud, they are not a substitute for criminal legislation. History has taught that criminals and the wireless industry are in an "arms race" where new technologies engender new criminal responses. To attack this criminal element requires new legislation to remove the need for law enforcement to prove intent to defraud when they find a suspect in possession of specialized cloning equipment—equipment that has no other purpose than to illegally clone wireless telephones. To this same end, we need legislation that makes clear that devices that intercept only the information necessary to illegally clone phones are defined as illegal scanners under law. Accordingly, we support the draft Wireless Telephone Protection Act, which was developed with close consultation between the United States Secret Service and the wireless industry.

While the wireless industry supports the draft Wireless Telephone Protection Act, we wish to point out that the bill focuses on cloning as it is practiced today, where a criminal uses a scanner and special software to fraudulently modify telecommunications instruments. Hardware and software that does not alter or modify a telecommunications instrument, but still permits fraudulent use, could fall outside the provisions of the bill. To address this problem, the bill could be amended to also prohibit the use, production, traffic in, control of, or possession of a program, information code, or command not provided by the manufacturer of a telecommunications instrument to originate or terminate commercial mobile radio service. To further broaden the protections of the bill, an additional amendment could make the replication of ESNs or MINs a violation of the counterfeiting and forgery provision of the US Code, which do not require showings of intent.

New legislation is also important because the telecommunications industry and the federal government are currently working to finalize the standards necessary to maintain the government's ability to conduct court-ordered electronic surveillance in the digital telecommunications age. Since criminals can often evade court-ordered surveillance via the use of cloned phones, it is imperative that Congress enact forward-looking anti-cloning legislation to give law enforcement greater ability, now and in the future, to stop this activity cold.

Mr. BARR. Thank you, Mr. Wheeler. Mr. Marinho, please.

STATEMENT OF JOHN MARINHO, CHAIRMAN, TR45 ENGINEERING COMMITTEE, TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Mr. MARINHO. Thank you, Mr. Chairman, and members of the Subcommittee. I am here before you today on behalf of the Telecommunications Industry Association (TIA) and in my capacity as Chairman of TIA's TR45 Engineering Committee. The TIA is a full service trade association of more than 600 members who manufacture and supply communications and information technology equipment and service throughout the U.S. and abroad; I might add edi-

torially that, to my knowledge, none of the manufacturers of the equipment that we have been talking about this morning.

The TR45 Engineering Committee is responsible for the wireless standards that serve most of the 50 Million subscribers that today are covered under the AMPS Family of Standards, which is a nomenclature that is commonly used to refer to the standards that are developed by the Engineering Committee.

The Committee is certainly very grateful for this opportunity to present testimony on the industry's efforts as mentioned earlier with regards to the technologies and standards that we have put in place relative to the detection and prevention of cloning and the fraudulent use of wireless telecommunications.

My comments again will focus on the activities of the TR45 Engineering Committee, but I will say that the TIA supports that CTIA's view as well as the comments made earlier by law enforcement relative to Congressional action regarding anti-cloning legislation.

To share with you a little bit of history, when cellular was first introduced in 1983 in the United States, based upon the AMPS Family of Standards, there were precautions that we took from a technology perspective relative to ensuring that the information that is key—that was mentioned earlier relative to the electronic information—was, in some sense, protected when it was transacted between the terminal and the network.

However, in the late 1980s and early 1990s, specialized scanning equipment materialized in the marketplaces, which we have heard earlier, with regards to being able to eavesdrop and prologue that information and then put it to inappropriate use. These initial standards and systems offered, again, a modest level of security but that only lasted for approximately 6 years so that the bandits could catch up.

With the mounting fraud, CTIA put in place requirements in 1992 relative to the development of new standards and technologies that would prevent the criminals from defrauding the network. And in 1992, TR45 embarked upon the development of these security standards. In 1994, this resulted in the sophisticated security set of standards and procedures that were mentioned earlier by Mr. Wheeler relative to the industry's standards for authentication relative to digital and analogue technologies.

These techniques are based upon relatively sophisticated cryptographic techniques that provide the authentication capability that defeats the ability for the cloned wireless terminal to mimic a legitimate subscribers' telephone. Today this represents the most powerful tool in the industry's arsenal against fraud. However, despite the fact that technology has made a theft of service increasingly difficult, the reality is that any system is prone to obsolescence, as was the system that we originally developed in 1983. That system lasted for approximately 6 years.

Within the Engineering Committee, we are now working on the next generation of security, algorithms and procedures, so that the industry can stay one step ahead of the criminals. However, given the cost that this represents to the industry, and the public at large in terms of constant mitigation for new standards and technologies, the TIA strongly supports Congressional action regarding

legislation to ensure that criminals are brought to justice and that penalties for convictions are stiffened.

In closing, and again on behalf of the TIA and the TR45 Engineering Committee, I would like to thank you for this opportunity and would be happy to answer any of your questions. Thank you.

[The prepared statement of Mr. Marinho follows:]

PREPARED STATEMENT OF JOHN A. MARINHO, CHAIRMAN, TR45 ENGINEERING COMMITTEE, TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Thank you, Mr. Chairman, and members of the Subcommittee. My name is John A. Marinho, and I am here today on behalf of the Telecommunications Industry Association (TIA) and in my capacity as Chairman of TIA's TR45 Engineering Committee.[1] TIA is a full service trade association of more than 600 members who manufacture and supply communications and information technology equipment and service throughout the U.S. and abroad. TIA represents both large and small companies which collectively provide the bulk of the physical plant and associated equipment for the industry. The TR45 Committee is responsible for the wireless standards that today serve most of the 50 Million subscribers in the United States of America. The committee is grateful for the opportunity to present testimony on the wireless industry's standards efforts regarding systems and technologies for the detection and prevention of criminal activities in the arena of cloning and the fraudulent use of wireless telecommunications services. My testimony will focus in particular on the activities of the TR45 Committee to address the industry's requirement for systems and technology that aid in the detection and prevention of cloning and fraudulent access. Additionally, the TIA supports the view of the Cellular Telecommunications Industry Association (CTIA) relative to Congressional action regarding the potential for forward-looking anti-cloning legislation.

CLONING & WIRELESS

When cellular service was first introduced in 1983, it was based on the standards which were established by the TR45 Engineering Committee. These standards were derived from the early work that had been done by AT&T and Bell Laboratories for the introduction of the Advanced Mobile Phone Service (AMPS) system prior to AT&T's divestiture. These standards are commonly referred to as the AMPS family of standards,[2] and have met the requirements of the American National Standards Institute (ANSI) to be issued as American National Standards. These standards today support over 50 Million Americans, and have also been adopted around the world in over 100 countries. Within the United States the AMPS standards have been deployed in the Cellular and Personal Communications Services (PCS) frequency bands,[3] and will form the basis for an evolution of AMPS to the next generation of wireless telecommunications.

The problem of wireless fraud first surfaced in the late 1980's and early 1990's when criminals began using specialized scanning equipment to intercept the unique identifying numbers that are associated with a wireless terminal and are communicated to the network across the air-interface during normal operation. These numbers are the Mobile Identification Number (MIN) and the Electronic Serial Number (ESN). The MIN typically represents the 10-digit telephone number that is assigned to the subscriber by the wireless service provider, and the ESN is the number that is assigned by the manufacturer of the terminal equipment. These two information elements are used by the network to uniquely identify the wireless terminal during normal operation relative to the placement and receipt of telephone calls.

The initial cellular air-interface standard that was defined for analog technology (i.e. ANSI Standard TIA/EIA–553), protected the MIN and ESN from eavesdropping

[1] Mr. Marinho is the Technology Director of Wireless Standards Development and Industry Relations, for Lucent Technologies Inc., of 600 Mountain Ave., Murray Hill, New Jersey, and has fulfilled the role as Chairman of the TR45 Engineering Committee since 1990.

[2] This family of standards represents a multiplicity of publications that address standards for the air-interface (i.e. connection between the wireless terminal and the network), intra-network and inter-network standards, security algorithms, speech coding algorithms, as well as standardized service descriptions. Examples of these standards include TIA/EIA–553, TIA/EIA–41, IS–136, IS–95, IS–634, IS–93, IS–124, etc.

[3] In addition to the AMPS Standards, the PCS 1900 Standards have also been deployed in the PCS Bands for licensed operation. The PCS 1900 Standards were established in the United States based on a derivative of the GSM Standards which were defined by the European Telecommunications Standards Institute (ETSI).

through digital transmission techniques[4] and a simple coding scheme to mask the MIN and ESN information. The industry became aware that criminals had begun to use specialized equipment to scan for and decode the digital information (i.e. MIN and ESN pairs) that would allow them to masquerade as legitimate subscribers. The masquerade is accomplished through the programming of a second wireless terminal with the information that had been intercepted from eavesdropping on the legitimate terminal during normal operation. Once the MIN and ESN information was duplicated in one, or more terminals, it was then not possible for the network equipment to distinguish between the legitimate and fraudulent terminal.

As the industry became increasingly aware of mounting losses attributable to cloning, requirements were put in place by the CTIA to address standard algorithms and procedures for enhanced security through the TIA's TR45 Committee. In addition to the standards related efforts, the industry also launched numerous non-standards based initiatives that served as an interim measure until the security standard was made available.

WIRELESS SECURITY STANDARDS

In 1992, in response to the requirements for enhanced security, the TR45 Committee embarked upon the establishment of standards that would provide for the ability to uniquely authenticate legitimate wireless terminals in light of fraudulent duplication of MIN and ESN information. This effort was undertaken by a subgroup within the TR45 Committee, referred to as the Ad-Hoc Authentication Group, that was comprised of recognized technical experts in the security arena. As a result of this activity, the standard for Authentication was defined as a network-wide cryptographic challenge and response mechanism that defeats the criminal's ability to successfully mimic a legitimate subscriber's wireless telephone.

The authentication capability is based upon standard cryptographic algorithms and the establishment of a "Key" information element which is known only to the service provider. This information element is referred to as the "A–Key" and is programmed into the wireless terminal and is also known by the network infrastructure. The A–Key is never transmitted across the air-interface, and is therefore not subject to eavesdropping or intercept, and is used for purposes of generating secondary key information that allows the network to interrogate/challenge the terminal equipment to determine legitimacy during normal operation. The secondary key information is referred to as the Shared Secret Data (SSD) and is used across the air-interface to authenticate the wireless terminal, as well as for detection of a cloning event.

The challenge is an instruction to the terminal, by the network, to calculate a response based on the transmitted SSD and the terminal's A–Key.[5] Once completed, the information is conveyed across the air-interface to the network where a comparison is done between the information provided by the terminal and the network's anticipated response. In the event that the comparison fails to be identical, the wireless terminal is deemed suspect and procedures to re-authenticate the legitimate terminal, as well as procedures to identify and pursue the fraudulent user may be implemented by the service provider. The process of re-authentication involves the re-generation of the SSD information by the network equipment in a random fashion. This process precludes the fraudulent, or cloned, terminal from having the ability to mimic a legitimate subscriber by eavesdropping on the SSD information that is transmitted across the air-interface. In essence, the standard authentication procedure has the ability to randomly re-key itself relative to the parameters that are exchanged over the air-interface. As a result, the cloned wireless terminal is unable to generate the appropriate response to the network's challenge.

In the event that the A–Key is compromised, by a fraudulent user gaining access to the corresponding MIN, ESN and A–Key information, the standard algorithm also provides for the ability to detect the presence of one or more cloned terminals. This ability in turn allows the service provider to take remedial action to identify the legitimate subscriber. Such action may entail operations personnel contacting the subscriber directly for purposes of confirming identity. It is likely that this situation would represent the minority of cases because the A–Key is not transmitted across the air-interface and is not accessible to the user.

The same authentication capability and procedures have been specified for the various standards within the AMPS family. The Authentication Standard was first published in 1994 with the introduction of the digital Time Division Multiple Access

[4] The transmission technique relies upon Frequency Shift Keying (FSK).

[5] Beyond the A–Key, other parameters are also involved, but are not specified herein for simplicity.

(TDMA) air-interface standard identified as IS–54 Revision B. Shortly thereafter, the same capability was specified in the analog TIA/EIA–553 standard, as well as for the digital Code Division Multiple Access (CDMA) standard identified as IS–95. Additionally, the necessary network signaling and protocol standards were specified in the TIA/EIA–41 standard that allows for support of authentication across the geographic boundaries of different service providers and networks. This capability provides for the same degree of security when a subscriber is roaming outside their Home network, as when they are within the coverage area of their Home network. In short, the Authentication capability of the AMPS family of standards represents the latest, and most powerful tool in the industry's arsenal against fraudulent access of the wireless network.

In addition to authentication, the standard also supports the capability to provide for the protection of user information through the privacy functions that support encryption of subscriber voice conversations or data transactions. This capability may operate in concert with the authentication system and protects the subscriber's information against unlawful eavesdropping at the air-interface. This privacy capability was defined to support the two digital air-interface standards mentioned previously (i.e., IS–136 TDMA and IS–95 CDMA), and provides for link encryption across the air-interface exclusively.

Once the authentication and privacy standards were completed and published, manufacturers and service providers quickly began the process to ensure that new systems and equipment would be capable of authentication. Nonetheless, tens of millions of non-authentication capable wireless terminals were in service prior to the establishment of the standards. These terminals remain in operation today and are subject to the threat of cloning. To address this situation, non-standard technologies and systems have been employed by service providers such as: Radio Frequency (RF) fingerprinting, usage profiling, Personal Identification Numbers (PINs), and others.

Despite the fact that technology and standards have made the theft of wireless service increasingly difficult for criminals, the reality is that any security system is prone to obsolescence after a period of time. In the same way that the original AMPS security approach was compromised after approximately 6 years, so too will the algorithms presently available to the industry be compromised at some time in the future. In light of this phenomenon, the TR45 Committee has put in place a work program to address the evolution of the standard so that the industry may stay one step ahead of the criminals relative to cloning and fraud. Enhanced security procedures and algorithms are being investigated through the work of the Ad-Hoc Authentication Group to ensure that the industry is prepared to move aggressively should today's authentication standard become obsolete through criminal activity. However, given the cost to the industry of fraud, as well as the cost of its constant mitigation through new enhanced standards and technologies, the TIA supports Congressional action regarding forward-looking anti-cloning legislation to ensure that criminals who clone wireless telephones are brought to justice and that the penalties for convictions are stiffened.

In closing, on behalf of the TIA and the TR45 Engineering Committee, I would like to thank the Chairman and members of the Subcommittee for this opportunity to provide testimony and for its ongoing assistance in fighting cloning fraud in the wireless industry.

Mr. BARR. Thank you, Mr. Marinho. Just to remove any confusion, the blue box there, Mr. Wheeler, you are saying that there is no legitimate use in the industry whatsoever for that?

Mr. WHEELER. No, sir. The only legitimate use is by law enforcement or in the industry. There is no use for a civilian other than to collect a number to clone into somebody else's phone.

Mr. BARR. Okay. I am just—that being the case, and I presume that yourself or somebody else from the industry could testify as an expert witness to that, I am still a little bit mystified as to why intent would be that hard to prove if there is, in fact, no use whatsoever other than for a law enforcement official or for a technician in the industry to possess that. I would think as a former prosecutor, it would be relatively simple to call an expert witness in and use that to establish the intent if you find some character out there with a bunch of these.

Mr. WHEELER. Mr. Barr, I think that this Committee and we thought that way in 1994 when the Act was expanded to include the intentional use of these devices to defraud, but the law has, instead, turned into a big loophole. Let me give you some examples. There was a case in the U.S. District Court in the Eastern District of Kentucky I believe, the *Yates* case, where this gentleman advertised in the newspaper, "Come to me, I will clone a phone for you so that you do not have to pay those additional bills," and he was arrested and brought to trial and he said, "Oh, I did not know that that was illegal." And the jury let him off because of the fact that there was no intent to defraud.

These people here are selling these devices which, again, have only one purpose and they are hiding behind the——

Mr. BARR. There are two purposes.

Mr. WHEELER. Two, correct. But they are hiding behind claims that it is for educational purposes; that it is not sold for the purpose of defrauding. I mean I have a hard time understanding what the educational purpose of this.

Mr. BARR. Where was this jury?

Mr. WHEELER. Pardon me?

Mr. BARR. Where was this jury? I hope not the Northern District of Georgia.

Mr. WHEELER. No, sir, it was in Kentucky. There are other cases in California where the court held that because of the fact that——

Mr. BARR. Well, we are well-aware of cases out in California.

Mr. WHEELER. I think the point is that there has had a chilling affect on what prosecutors have been willing to do. I mean that clearly was not the intent of Congress, as you just indicated, but the fact—I mean here is a book full of people who get away with it. Here are the folks on the Internet who, everyday, are driving through that loophole by saying, "Oh, we are not doing this with an intent to defraud." I mean, they were——

Mr. BARR. Have there not been successful prosecutions under circumstances similar to this one where the jury let the fellow off?

Mr. WHEELER. The answer to that is yes, but unfortunately they often come under the guise of then prosecuting for something else. As a matter of fact, I think there are multiple benefits that come from addressing the intent problem:

One is that you can shut down the early and easy access like this. The second is that it encourages law enforcement to go against the offenders rather than the current situation which is a discouragement, "Oh, my gosh, I have these other precedents over here." And thirdly, it becomes another arrow in the quiver of law enforcement, if you will; if you cannot get Al Capone on racketeering maybe you can get him on tax evasion. If you cannot get these drug dealers on one issue, then the fact that they have this device is a hook and there is only one reason why they have it.

There was recently a case that has not come to trial yet, but the Russian Mafia—people involved in the Russian Mafia—were sitting in an apartment in the Bronx and had collected 80,000 electronic ID numbers from cars going on the Cross-Bronx Expressway. 80,000! Now, there is not a reason why you have 80,000 numbers. The problem is, how do you then connect from having this device to actually going to get the intent and those 80,000, by the way,

were discovered by accident when they were there for something else.

Mr. BARR. And that gets to sort of another part of the problem again. Even if the statute were modified and made even to lower the threshold even more than in Mr. Johnson's Bill that has been or is going to be introduced, I mean that still is not going to solve all of the problems; even if we made the simple possession without any showing of intent. You know, luck plays a role. I presume that with this fellow that was doing that there were other things they could have gotten him on.

And, again, maybe we have unusual juries and judges and prosecutors in Georgia, but we would prosecute—I was the U.S. Attorney before these new laws—but we would prosecute people based on similar writings in magazines, whether it is a Soldier of Fortune magazine or something else, on a fairly regular basis.

I am not saying that we should not look at changing the statute. I think a lot of the problem may be, you know, certain prosecutions, law enforcement priorities, where juries every now and then and certainly that one word "jury" is the only that is going to get blasted all over the Internet and throughout the industry and that is—I do not know that there is anything we can do about that.

Let me shift the focus, if I could, just for a moment when we had the law enforcement folks on the previous panel as you both heard. We got into a brief discussion of what is it that industry could be doing to meet the threat of the ever-increasing technological capabilities of the bad guys? What is there—and if you could discuss it a little bit in terms of the time that it takes to develop this technology and the cost of it.

Mr. WHEELER. Let me ask my colleagues to put up some graphics. This is four quick examples of things that we are doing right now, kind of in an evolutionary process. In the upper left hand corner is a profiling technology which we borrowed from the credit card industry. You know that if you take your Visa card and you use it in New York at 3:00 and somebody uses it down in Atlanta at 4:00, that 4:00 one is not going to get authorized because you cannot get there in time and it is a fraudulent card. Likewise, we are in a similar situation: You cannot use a phone in New York and Atlanta back-to-back that quickly and so we run profiles and we say, "This does not make sense. Therefore, this must be a fraudulent call," and we shut that call down and then begin to roll up the chain. So that is one thing that has been done.

A second is to use PIN technology and what is called roamer verification. You saw in those highlighted numbers right there that Secret Service Agent Riley showed how they were capturing the PIN off of the air by this device as well. Therefore, unfortunately when we put in the aggravating requirement to add your PIN after you have dialed the number—the bad guys got around that real quickly. So that is one that has worked temporarily but was only a temporary fix.

Interestingly, two other things that are going on are technologies which we have taken from defense industry. One is RF fingerprinting. It turns out that every radio has its own unique finger print; the way that the antenna is bent , where there are scratches or whatever the case may be means that the wave form

comes out slightly different. So we are installing technology now that says "This is Mr. Barr's legitimate wave form," and we will relate that to his electronic serial numbers and if those two match the call goes through. But if I try and use your identification numbers, then it comes up with my wave form and says "No, those two do not match." It is a cloned phone and shuts it down. That has been very, very effective.

Mr. BARR. How much margin for error in there is there? Would the gentleman from Arkansas allow us a little discretion in terms of time? I do not want to infringe on his time. But for example, if I take my phone, as I will do sometimes, and if I am driving my wife's car, put it in her car and use it; the signature, because the car is maybe slightly different, as you say, the antennas or whatnot may be different, it may give a slightly different signature. Would that mean that my call would be blocked even though it is me trying to use it simply on another car?

Mr. WHEELER. Good question. No, because the way you come up with what the signature is is by doing a study over a lengthy period of time. You say, okay, the Barr ESN/MIN pair is coming from phones which look like what, and so that would be in the record. However, if suddenly the new one pops up, then you say, something is wrong. So very good question.

The other thing that is going on, and John Marinho has been very involved in, is authentication. And that is that there is a query response between the system and the phone, where the system will query the phone which has to give the right kind of a algorithm response or else it does not work. Now, you should know that we at CTIA run a—for lack of a better description—underwriters lab certification program for phones.

It is a requirement that for a phone to get the CTIA certification seal it has to have this authentication capability built in. And so for instance, when the FBI representative was saying that the industry should do something, I would submit that we have. This technology has now been built in and what is more, it will not get the seal of approval—which is the precursor to buying the unit because the industry knows these are good units—unless it does have this authentication.

Now, this is all the good news on the picture, if you will. And what this does is it makes it more difficult for the guys who buy these, but everything can be done—for every code there is a decode, if you will. And that is what I meant by the arms race. Because what this does is to shut down the casual cloner, the amateur, if you will.

There is a serious business of cloning labs; professional folks who use this for the sole purpose of cloning. They have an economic incentive to find the way around this and then we will have to play catchup ball with them again. So what I think we are suggesting, Mr. Barr, is that we are ready to engage in that arms race, if you will, but that it is not just technology alone, that the law has to back up the technology, and the law has to make it clear that this device will not have the kind of loopholes like educational applications, and "I promise I will not defraud" that allows it to be sold today.

Mr. BARR. Thank you, Mr. Wheeler. The gentleman from Arkansas is recognized.

Mr. HUTCHINSON. Thank you, Mr. Chairman. Mr. Wheeler, following up on that, the cellular telephone industry obviously is concerned about their own economics here and the previous witnesses, the FBI, the DEA, Secret Service, are very concerned about the use of cloned telephone devices for drug trafficking. Of course, the industry's concern, as well as for the public good, would be a concern about their own industry and their economic damage. How much money does the cellular telephone industry lose each year in lost revenue from cloned telephones?

Mr. WHEELER. Well, there is good news and bad news in that answer. The bad news is that it is hundreds of millions of dollars. The good news is that, while the trend line had been going like this, it has started to go like this because of the implementation of these technologies.

Mr. HUTCHINSON. But it would be hundreds of billions of dollars you said?

Mr. WHEELER. Hundreds of millions.

Mr. HUTCHINSON. Millions of dollars. Now, you indicated that new technology that you develop will stop the amateurs but not the professionals. I assume that these professionals acquire these numbers and clone a phone and then sell the phone or do they sell the numbers?

Mr. WHEELER. Both.

Mr. HUTCHINSON. And who is their market?

Mr. WHEELER. The next step in the criminal food chain. They are the people who go out and use this invisibility, which a cloned phone gives them, to perpetrate another crime. So it is one crime; the cloning, aiding and abetting and permitting the perpetration of yet another and, frankly, more heinous crime.

Mr. HUTCHINSON. And so the drug dealer himself might not be cloning a phone but he might be purchasing a cloned phone from one of these professionals that you refer to.

Mr. WHEELER. Yes, sir.

Mr. HUTCHINSON. And so the professionals could be selling to someone who is engaged in illegal drug trafficking or it could be some other type of illegal behavior.

Mr. WHEELER. Yes, sir.

Mr. HUTCHINSON. Or it could simply be for the economic crime of being able to use long distance calls free of charge.

Mr. WHEELER. Yes, sir.

Mr. HUTCHINSON. Now, you also indicated that you are preparing for an arms race and one of the tools you want to use is a revised statute that deletes the intent requirement and makes simple possession a crime. You indicated that if this happens, criminals will hack the network next.

Mr. WHEELER. Right.

Mr. HUTCHINSON. Would you explain that? I am not sure what you mean by the network.

Mr. WHEELER. A cellular phone network, or wireless phone network, is nothing more than the interconnection of a whole series of computers that will say, for instance, "Mr. Hutchinson's phone is leaving my area. Is there another antenna that picks it up," and

we will switch it off to where that interconnects with the switch in the landline network which is nothing more than a computer itself. It is just a network of computers.

The reason that cloners today use this and go against the phone is it is the weakest link, and if we shore that up—when we shore that up—with law and technology, I do not think they are just going to throw up their hands and say, "Well, they have beaten us." They are going to say, "Okay, now, what do I do next? Where can I go next?"

If these same mentalities hack into bank records and hack into the Defense Department and everything else—then hacking into the wireless network similarly is not that great a challenge for them. What we do not want to do, however, is to drive them to do that and then find out that this statute or something else drove them to do that and there is no statute that says they cannot do that.

And so what I am trying to say is, "How do we think like a Chess game?" How do we think a couple of moves ahead on the bad guys so that they are responding to us instead of us responding to them. As I said, in 1994, this Congress passed a law that we all thought solved the problem. Here we are back today responding to the bad guys who are driving through a loophole in that law. Let us hope we do not come back in three more years and say, "Well, now, we have got to respond to their next initiative." Let us see if we can get out in front of them.

Mr. HUTCHINSON. Well, I agree with you and I think it is important to address this legislatively. I think it is important to carefully craft the law to provide the proper exceptions to make sure that we do not infringe upon an individual's rights. That is the purpose of this hearing and I congratulate the chair for his very appropriate questions and I thank the witnesses. I yield back the balance of my time.

Mr. BARR. Thank you, Mr. Hutchinson. Just one final question that I had. Mr. Marinho, the cell-phone that I have is not digital. I know there is new technology coming on the market; digital phones. Is that a direction that we should be looking at, and also from a technological standpoint—and I say this as somebody that does not know a lot about the technical aspects of this—is there any sort of very easy way to dis-scramble the signal so that somebody, you know, cannot just pick it up with one of these scanners? Could you just comment on those two aspects, please?

Mr. MARINHO. Certainly. With regards to your comment regarding digital, certainly the digital technology makes it much more difficult for the would be, or even in some cases sophisticated hacker, to be able to eavesdrop on the technology in terms of the transactions that go on between the terminal and the network. However, that in and of itself is not sufficient and is the reason why we have employed encryption technologies and encryption techniques to encrypt the information so that it, in some sense, is not prone to being eavesdropped when it is transacted between the terminal and the network relative to the authentication process that was mentioned earlier.

However, in addition to employing these techniques for the digital technology, the analogue phones that are also certified by the

CTIA because you can buy both varieties today; both analogue and digital, also have the same capability in terms of authentication. They do not have the ability in terms of the user's voice privacy because it was not practical from a manufacturing standpoint to do that for the analogue technology. However, it is available in the digital technology in terms of encrypting the user's voice as well as encrypting the user's data should they choose to transact data on the digital channels that you can utilize with the digital phone.

Mr. BARR. When you talk about encryption, are you talking about something where—for example, my existing phone, which is several years old, would I have to bring that unit in and have something done to it or the transmission box in the car, or is that something that would be done at Bell South for example?

Mr. MARINHO. The phones that are purchased on the market today, that are certified by the CTIA, are complying with the standard and regardless of whether they are digital or analogue will have the authentication capability in them. However, phones that were manufactured and deployed in the network prior to the establishment of the standard do not have the benefit of that capability and those are the phones that are prone to being cloned because of the fact that we only introduced the standard in 1994.

But the other methods that were mentioned by Mr. Wheeler with regards to profiling, PIN verification, et cetera, are effective means to address that population of telephones that are out there and it is anticipated that over the course of time those phones will be, in some sense, replaced with new phones, given the life cycle that technology goes through.

Mr. BARR. So to some extent, and I do not want to certainly not minimize the problems that we now face and that we are facing with these people, but to some extent the problem will take care of itself as digital phones become more—the price comes down as supply increases and so forth and as some of the older phones, perhaps such as mine, are traded in for a new unit and so forth. So that, I presume, is a little bit of good news down the road; would that be fair?

Mr. MARINHO. I think that that is a fair comment. However, I think what we have done so far is to just cause a change in the curve that Mr. Wheeler mentioned earlier in terms of defeating the ever increasing problem. However, if we do not have the legislation that, in some sense, backs up what the industry is trying to do, in terms of effectively making it a very serious penalty for the commission of that particular type of crime, I think we will very easily run into the same situation maybe 6 years or 8 years from now or maybe even sooner because, again, if it took them 6 years to break the first technology that we had out there, it is very likely that it will take them even less time to break the second.

So I think that even though we are trying to stay one step ahead of the criminals, I think that the linkage to the legislation is a very important one so that, again, we can heighten the sensitivity of the public, particularly the criminals, relative to penalties associated for committing this kind of crime. And again, I would echo the comments made earlier that there is no reason for anybody to need this equipment other than organizations that are in the industry or law enforcement.

Mr. BARR. Thank you. Mr. Hutchinson, anything else?

I would like to thank both of you gentlemen for being with us today and if there is any additional material, both today or at any time in the future that you would like to submit to us, please feel free to do so because as we work through this process of trying to come up with, as Mr. Hutchinson said, laws that balance the privacy needs and the cost to industry by creating mandates verses legitimate law enforcement needs, we welcome and need the input from business and industry. We appreciate your continued interest in that. Thank you. This hearing is concluded.

[Whereupon, at 11:15 a.m., the Subcommittee adjourned.]

○

55-946 (96)