Telecommunications Overview

Advanced Telephony Unit
Federal Bureau of Investigation
Purpose

To Provide an Overview of the Telecommunications Environment and its Implications for Law Enforcement
IMPACT OF EMERGING TELECOMMUNICATIONS TECHNOLOGY ON LAW ENFORCEMENT

- The Nation’s telecommunications systems and networks are often used in furtherance of serious criminal activities.

- Recent and continuing advances in telecommunications technology and the introduction of new technologies and transmission modes have made it increasingly difficult for Federal, State and local law enforcement agencies to enforce the criminal law through a key investigative technique--statutory-based, court ordered electronic surveillance.
CHALLENGE TO LAW ENFORCEMENT

These technologies present a two-fold challenge to law enforcement:

1) The ability to access communications subject to court authorized intercepts (Digital Telephony Legislation); and

2) The ability to gather and analyze evidence from these interceptions on a real-time basis (National Encryption Policy Issue).
LEGISLATIVE HISTORY

In 1968, Congress, after carefully considering the constitutional issues between the Government’s need to effectively investigate serious criminal conduct and an individual’s right to privacy, passed the Omnibus Crime Control and Safe Streets Act. (Amended in 1986 - Electronic Communications Privacy Act - 18USC2510.)

This established a procedure for law enforcement to obtain judicial authorization to conduct electronic surveillance.
LEGISLATIVE HISTORY (CONTINUED)

- Thirty-seven states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted similar legislation authorizing state and local law enforcement agencies to conduct court authorized intercepts.

- Foreign Intelligence Surveillance Act (FISA) 50USC1801, passed by the Congress in 1978.
<table>
<thead>
<tr>
<th>Year</th>
<th>Original Interception Applications Authorized</th>
<th>Reported Results</th>
<th>Arrests</th>
<th>Convictions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>State</td>
<td>Federal</td>
<td>Total</td>
<td></td>
</tr>
<tr>
<td>1982</td>
<td>448</td>
<td>130</td>
<td>578</td>
<td></td>
</tr>
<tr>
<td>1983</td>
<td>440</td>
<td>208</td>
<td>648</td>
<td></td>
</tr>
<tr>
<td>1984</td>
<td>512</td>
<td>289</td>
<td>801</td>
<td></td>
</tr>
<tr>
<td>1985</td>
<td>541</td>
<td>243</td>
<td>784</td>
<td></td>
</tr>
<tr>
<td>1986</td>
<td>504</td>
<td>250</td>
<td>754</td>
<td></td>
</tr>
<tr>
<td>1987</td>
<td>437</td>
<td>236</td>
<td>673</td>
<td></td>
</tr>
<tr>
<td>1988</td>
<td>445</td>
<td>293</td>
<td>738</td>
<td></td>
</tr>
<tr>
<td>1989</td>
<td>453</td>
<td>310</td>
<td>763</td>
<td></td>
</tr>
<tr>
<td>1990</td>
<td>548</td>
<td>324</td>
<td>872</td>
<td></td>
</tr>
<tr>
<td>1991</td>
<td>500</td>
<td>356</td>
<td>856</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>4,828</td>
<td></td>
<td>2,639</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7,467</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>35,851</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>19,259</td>
<td></td>
</tr>
</tbody>
</table>
BENEFITS OF ELECTRONIC SURVEILLANCE

- To illustrate the impact of this extremely important investigative technique, during the period of 1985 to 1991, court authorized intercepts conducted only by the FBI for criminal investigation only led to:

  - 7,324 individuals convicted;
  - $295,851,162 in fines being levied;
  - $756,363,288 in court ordered recoveries, restitutions and forfeitures; and
  - $1,862,414,937 in prevented potential economic loss.
THE THREAT TO LAW ENFORCEMENT
DIGITAL TELEPHONY

Emerging technologies and intelligent networks are being developed and implemented throughout the telecommunications industry without apparent consideration to the legitimate needs of law enforcement.

Without mandated assistance of electronic communications services providers, law enforcement cannot be assured access to the communications identified in the court order.
THE THREAT TO LAW ENFORCEMENT DIGITAL TELEPHONY (CONTINUED)

- Information obtained from these intercepts has:

  (a) helped to prevent the death or physical injury of innocent victims,

  (b) thwarted violent criminal activity, and

  (c) provided extremely credible, persuasive evidence in prosecution of these cases.
I. THE CURRENT ANALOG ENVIRONMENT.

II. THE NEW TELECOMMUNICATIONS TECHNOLOGIES:

* ARE NOT EXPERIMENTAL;
* ARE BEING DEPLOYED COMMERCIA 者;
Today's Operational Environment

Analog Transmission

2-wire Connection
Distribution Cable
Feeder Cable

Residence
Pedestal
Serving Area Interface
Central Office

Digital Transmission
Leased T1 Facilities (copper)
MUX
Fiber Optic Facilities

Business
Central Office
Integrated Services Digital Network (ISDN)

- Telephone
- Data terminal
- PBX
- Alarm
- Customer ISDN Interface
- "Digital pipe"
- ISDN central office
- Local area networks (LANs)
- Packet-switched network
- Circuit-switched network
- Other networks
- Data bases
- Other services
Personal Communications Services (PCS)

Callers Dial Your PCS Number and the System Forwards Their Calls to You at Several Locations Simultaneously.

PUBLIC NETWORK

PSN Switch

Subscriber Database

Voice Mail

When No Answer, PCS Transfers to Voice Mail

...To Where You Work

...To Your Home

...To Your Mobile Phone

Change the Direction of Your Calls From Any Touch-Tone Phone.
Follow-Me Services

AT&T Easy-Reach Service
- One 700 Number for Life
- Calls Follow You When You Move
- Customized Telephone Numbers Available
- Selective Call Forwarding Capabilities
- Programmable From Any Touch-Tone Phone

(415) 555-1111
(700) REACH ME
(202) 555-2222
The Emergence of Alternate Access Providers Is Increasing the Number of Players in the Local Exchange
THE PROPOSED LEGISLATIVE SOLUTION FOR DIGITAL TELEPHONY

The purpose of this proposal is to clarify the responsibilities of the providers of electronic communication services when providing law enforcement with the "technical assistance necessary to accomplish the interception," as required by Title 18, U.S.C., Section 2518(4) and Title 18, U.S.C., Section 3124(a)(b) and to set reasonable time frames for compliance.
NATIONAL POLICY ON ENCRYPTION
The Threat Facing Law Enforcement Encryption

The challenge facing law enforcement is the ability to understand the contents of intercepted communications in a real-time manner. Technology advances in the telecommunications industry will facilitate the development and production of affordable, superior voice quality, cryptographically excellent encryption devices for voice, data, and image transmissions.
Encryption Equipment

- Growth in Data Encryption Equipment Market Will Be Spurred By Increases In:
  - Networking
  - Legal Mandates for Security
  - Commercial Espionage
  - Resolution of Standards Issues

- US Data Encryption Equipment Market Will Reach $443 Million in 1992 and $946 Million By 1996

Source: Digital Review

Source: Advanced Telephony Unit, FBI
SECRET

NEED FOR A NATIONAL POLICY:

0 Although the export of encryption products within the United States is controlled, its domestic use is not regulated. A policy is needed which embodies national legislation, which:

0 Affords legitimate users of cryptography protection which their adversaries cannot defeat.

0 Insures that cryptographic devices and systems are capable of real-time decryption by law enforcement.

0 Prohibits cryptography that cannot meet the standard enumerated above.

0 An exception will, of course, exist for the protection of classified National Defense Information.
RATIONALE FOR DECRYPTION ABILITY BY LAW ENFORCEMENT

0 The protection of a citizen’s possessions against unreasonable searches and seizures is guaranteed by the Constitution.

0 This does not, however, prohibit court authorized searches performed by law enforcement officers, based upon probable cause (e.g., reasonable belief grounded on facts).
RATIONALE FOR DECRYPTION
Ability
By Law Enforcement (continued)

0 When Congress and state legislatures granted court authorized interception they intended that it be available in all circumstances.

0 To permit unregulated use of excellent cryptography would establish an electronic sanctuary for conducting criminal activities, unfettered by legal process.