

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 11-24-2008 BY 60322/UCLRP/PJ/EHL

NATIONAL LAWFUL INTERCEPT STRATEGY

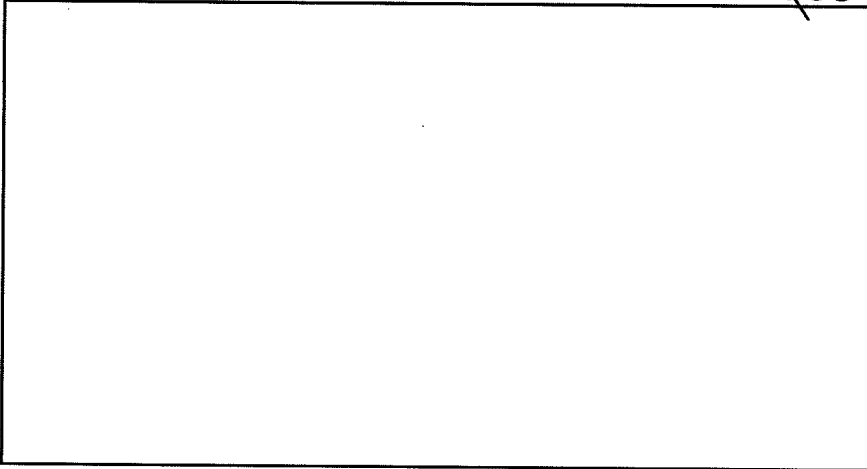
Current and Future Challenges

Operational Technology Division



LAWFUL INTERCEPT CAPABILITIES ARE ERODING AND AT RISK OF GOING DARK

- Existing trends indicate the FBI will have substantial and wide spread electronic surveillance difficulties in 2 to 3 years



b2
b7E

- Stable communication environment from time telephone invented in 1876 until 1983 - Alexander Graham Bell

MULTIPLE ACCESS METHODS TO A VARIETY OF SERVICES

Home

Work

Mobile

Travel

Municipal Wi-Fi Access or other Hotspot

EarthLink

NETZERO

BlackBerry

comcast

Sprint

at&t

Any of a number of providers

Kazaa

napster

Xdrive

AIM.com

AOL

skype

Yahoo!

dailymotion

Hotmail

FBI - Operational Technology Division

5

ALWAYS ON, ALWAYS CONNECTED, ALWAYS MOVING WIRELESS SERVICES / CAPABILITIES



- 2.5G (GPRS)
- 3G (UMTS)
- Wi-Fi
- Bluetooth
- GPS
- 3rd Party Applications
- Camera
- Keyboard
- Touch Screen
- Price (with contract)

iPhone



\$499.99

Cingular 8525



\$299.99

Blackberry Curve



\$199.99

Samsung Blackjack



\$99.99

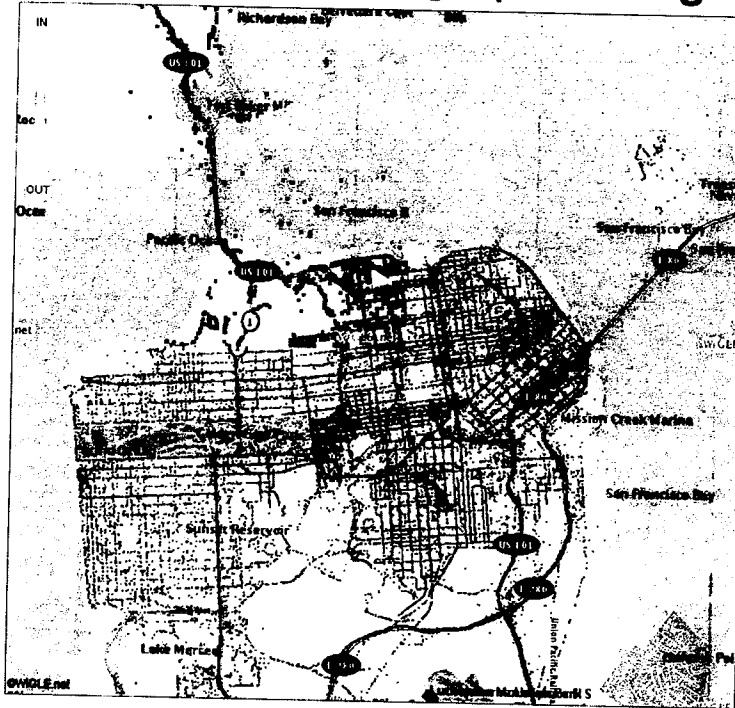
..T..Mobile..

	T-Mobile			
	BlackBerry 8800	Sidewick 8	BlackBerry Pearl	Dash
2.5G (GPRS)	T	T	T	T
3G (UMTS)	T	T	T	T
Wi-Fi				T
Bluetooth	T	T	T	T
GPS	T	T	T	T
3rd Party Applications	T	T	T	T
Camera	T	T	T	T
Keyboard	T	T	T	T
Touch Screen				T
Price (with contract)	\$349.99	\$199.99	\$149.99	\$149.99

FBI - Operational Technology Division

WI-FI OVERVIEW

San Francisco Coverage (from Wigle.net)

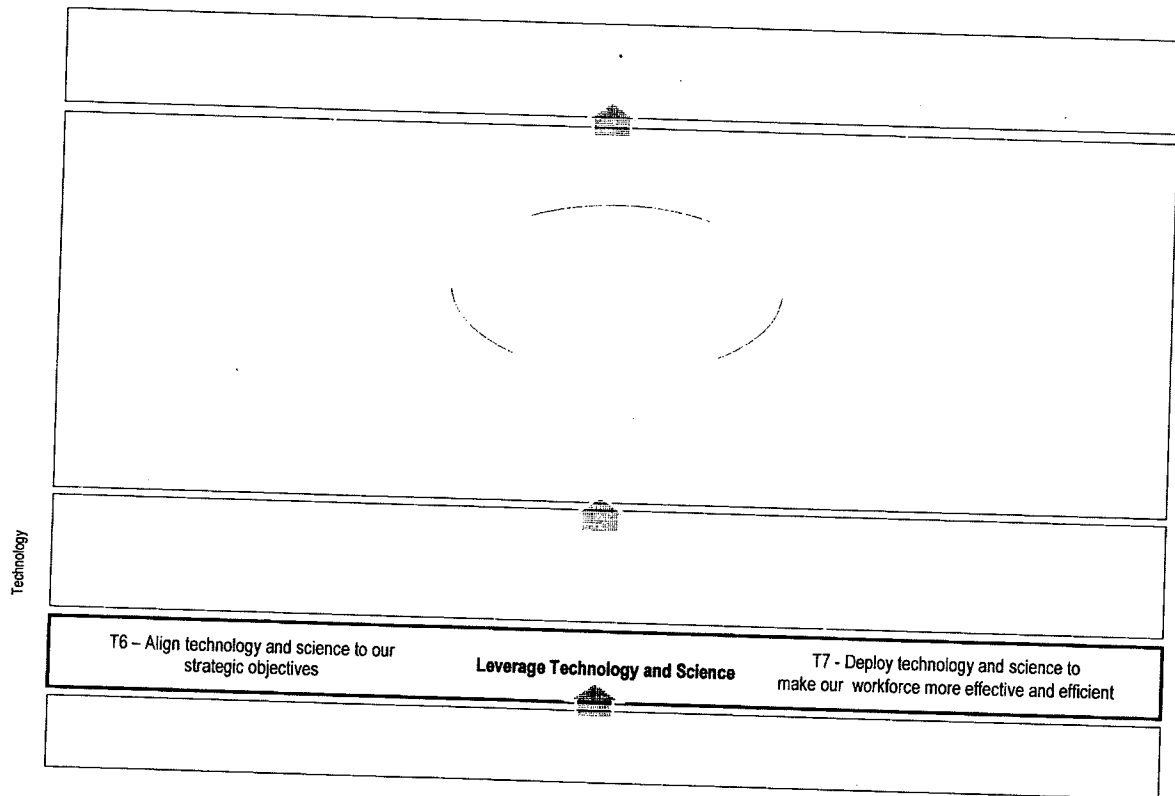


A BLETCHLEY PARK APPROACH TO THE PROBLEM



FBI - Operational Technology Division

ELECTRONIC SURVEILLANCE IS A FOUNDATION OF THE FBI'S STRATEGIC FRAMEWORK



BACKUP MATERIAL

NATIONAL LAWFUL INTERCEPT STRATEGY

- Enhanced cooperation between law enforcement and industry
- Enhanced cooperation and coordination across the law enforcement community (National Lawful Intercept Coordination Center)
- Updated authorities (Protection of sensitive/proprietary information from industry etc.)
- Update legal mandates (CALEA etc.)
- Adequate resources and infrastructure for the law enforcement community

NATIONAL LAWFUL INTERCEPT STRATEGY

Current and Future Challenges

Operational Technology Division

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 11-24-2008 BY 60322/UCIRP/PJ/EHL





**COMMUNICATIONS ASSISTANCE FOR LAW
ENFORCEMENT ACT (CALEA)**

ITSG Workshop

Section Chief Michael P. Clifford, Jr.

Electronic Surveillance Technology Section

Federal Bureau of Investigation

April 21, 2004

AGENDA

Electronic Surveillance Background

CALEA Background and Progress

Regulatory Uncertainty and the Petition

Need for Standardized Solutions

DEFINITION OF ELECTRONIC SURVEILLANCE

A law enforcement tool whereby officers acting pursuant to lawful authority are permitted to use a device to overhear and record conversations or other transfers of information

Examples include wiretaps, acquisition of information about calls (pen register / trap and trace devices), microphones, and closed circuit television

HISTORICAL PERSPECTIVE

Fourth Amendment

- Unreasonable searches and seizures

- Probable cause

- Particularly describing the place to be searched

1914 - *Weeks vs. U.S.*

- Exclusionary rule

1928 - *Olmstead vs. U.S.*

- "Trespass" view

1934 - Federal Communications Act § 605

- Did not properly regulate

- Did not provide for a method of using information in court

HISTORICAL PERSPECTIVE (cont'd)

1967 - *Berger vs. New York*

- Probable cause

- Particular description (communications seized and phone line)

- Time limit

1967 - *Katz vs. U.S.*

- Katz overturned *Olmstead*

1968 - Omnibus Crime Control & Safe Streets Act ("Title III")

- Federal wiretap statute

1970 - Amendment to Title III

- Service providers must supply all technical information, facilities, and assistance necessary

HISTORICAL PERSPECTIVE (cont'd)

1977 - *U.S. vs. New York Telephone*

“Any assistance necessary to accomplish an electronic interception”
No obligation for carriers to design equipment to facilitate authorized electronic surveillance

1986 - Electronic Communications Privacy Act (ECPA)

E-mail, facsimiles, display pagers, cellular telephones
Stored communications and transactional records
Pen registers and trap and trace devices
“Roving” wiretaps

1994 – CALEA

Affirmative obligation to design equipment to facilitate surveillance

TITLE III: KEY DEFINITIONS

“Intercept” - acquiring contents of a communication using a device

“Contents” - substance purport or meaning of a communication

“Wire communication”

Involving the human voice

At least partly through use of a wire

Includes transmission through a “switching station”

Includes “electronic storage” of a communication

TITLE III: KEY DEFINITIONS (cont'd)

“Electronic communication” - any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature, transmitted in whole or in part by wire, radio, electromagnetic, photoelectronic, or photooptical system except:

- A wire or oral communication
- Tone only paging device
- Tracking device
- Electronic funds transfer

LIMITS OF TITLE III COVERAGE

No person may “intercept” nor use nor disclose the “contents” of any “wire, oral or electronic communication” except as otherwise provided in this statute

Criminal and Civil penalties

Exclusionary rule applies

Exceptions

- Service provider course of business

- Certain FCC monitoring responsibilities

- Consent by one party

- Electronic and radio communications readily accessible to the public

- Pen register and trap and trace devices

PEN REGISTER AND TRAP AND TRACE ORDERS

Smith vs. Maryland (1979)

Electronic Communications Privacy Act (1986)

Acquire outgoing (pen) and incoming (trap) dialing and signaling

Legal requirements for use

Attorney for the government certifies, in writing and under oath, that the information likely to be obtained is relevant to an ongoing criminal investigation

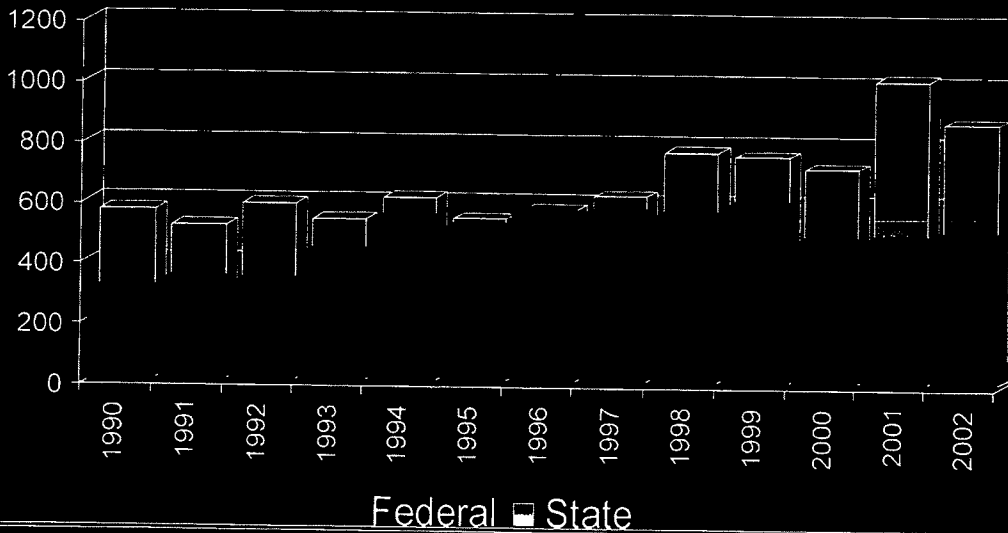
No probable cause requirement

Magistrate must issue order

TITLE III WIRETAP AUTHORIZATIONS 1990-2002

In 2001, State and Local law enforcement wiretaps outnumbered Federal by a 2:1 ratio

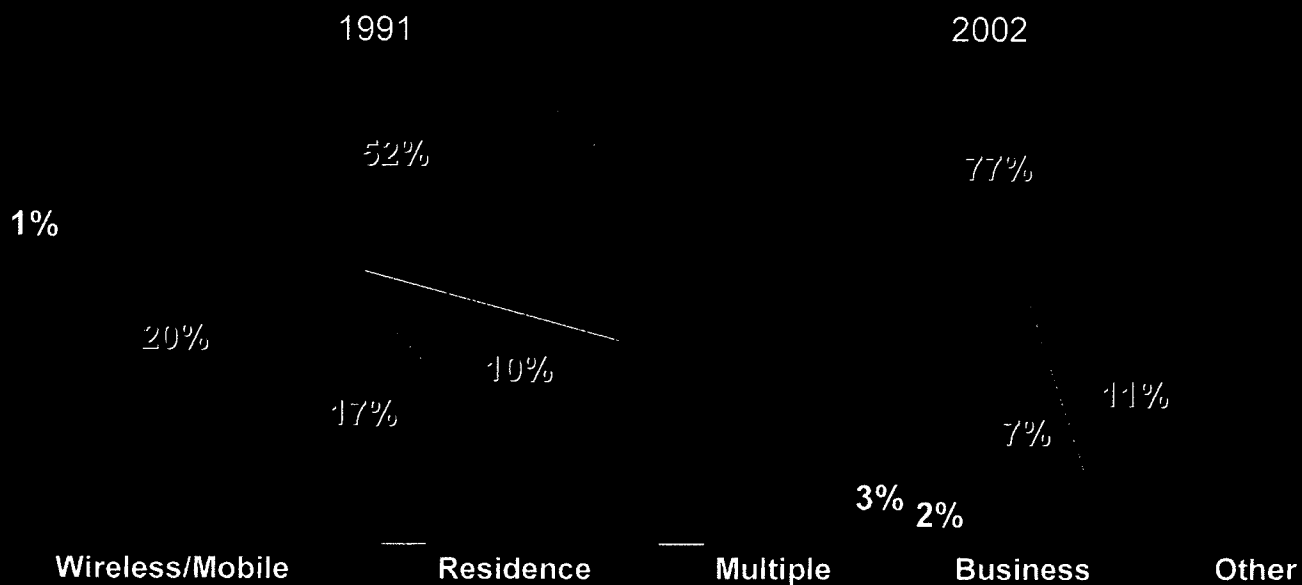
Only in 1996, did Federal wiretaps equal those of State and Local law enforcement (i.e., 1:1 ratio)



WHERE TITLE III WIRETAP AUTHORIZATIONS OCCUR

Shift in location of wiretaps

Importance of electronic surveillance of wireless / mobile



CALEA BACKGROUND

CALEA was enacted in 1994 responding to 1980's technological changes that limited law enforcement's ability to conduct electronic surveillance despite having statutory authority

CALEA does not apply to a specific technology, but rather covers all forms of telecommunications and is technology-neutral

The intent of CALEA was to be forward-looking and put industry on notice with respect to future services and law enforcement's electronic surveillance needs

CALEA , THE RESULT OF 1980's TECHNOLOGICAL CHANGES

1980's technological changes introduced services that threatened or eliminated law enforcement's ability to conduct electronic surveillance:

- Call forwarding
- Call transfer
- Multi-party calling
- Calling Cards

CALEA: FORWARD-LOOKING LEGISLATION

CALEA requirements are not static and do not apply only to technology available at the time of enactment

Legislative history clearly states that service providers are to:

“ . . . ensure that new technologies and services do not hinder law enforcement access to the communications of a subscriber who is the subject of a court order authorizing electronic surveillance.”

Telecommunications services are quickly migrating to packet networks designed to carry Internet traffic with little or no ability to facilitate electronic surveillance

WHAT IS CALEA ABOUT?

CALEA is about **ACCESS** not *AUTHORITY*

The intent of CALEA is to ensure that law enforcement has the capability to intercept all call content and call-identifying information coming from or directed to the telecommunications instrument that is the subject of a lawfully-authorized electronic surveillance

CALEA Implementation . . . A sample of what has been done to date . . .

CALEA IMPLEMENTATION PROGRESS – TRADITIONAL TELECOMMUNICATIONS SERVICES

Finalization of the industry's first electronic surveillance standard: J-STD-025, FCC, and Court rulings

Nationwide Right-to-Use (RTU) software license agreements making technical solutions available

Enhanced capability to lower law enforcement's delivery costs and virtually eliminate facility-based delay

Flexible deployment to significantly lower the burden on small, rural service providers

CALEA IMPLEMENTATION PROGRESS – OTHER TELECOMMUNICATIONS SERVICES

Deployment of technical capabilities in many wireless networks

FBI participation in a variety of industry-sponsored standards-setting organizations allowing it to influence the design of technical capabilities

Development of law enforcement requirements for next-generation services

- Packet Surveillance Fundamental Needs

- Carrier Grade Voice over Packet

- Public Internet Protocol Network Access Services

TECHNOLOGICAL CONVERGENCE IS OCCURRING AT AN UNPRECEDENTED PACE

Wireless mobile development and deployment will accelerate over the next few years

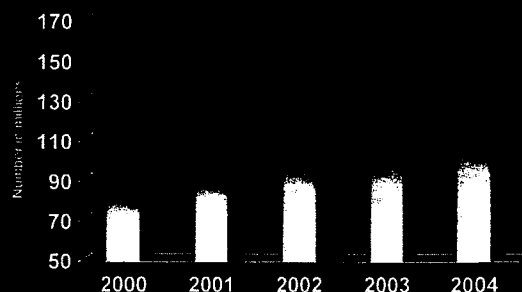
Service providers will release new services to:

- Increase customer loyalty and reduce churn

- Gain additional revenue from existing subscribers

- Attract new subscribers

- Reduce expenses

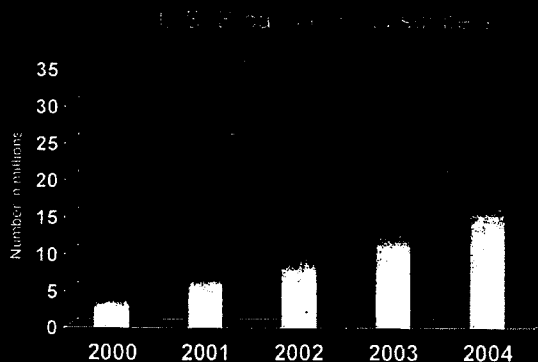


Convergence is bringing together Internet and wireless environments blurring the “service” distinction

TECHNOLOGICAL CONVERGENCE IS OCCURRING AT AN UNPRECEDENTED PACE (cont'd)

Broadband subscribers, led by cable modem and DSL, grew from almost 19 million in 2002 to more than 26 million in 2003

Subscribers are expected to increase to more than 60 million in 2008



REGULATORY UNCERTAINTY

Minnesota PUC ruling Vonage is a telecommunications service - District Court over-ruled MPUC

States opening rulemakings to determine regulatory status of Internet-based communications

FCC Wireline and Cable Modem Internet Access Proceedings and the Ninth Circuit's remand of the FCC

FCC's recent decision declaring pulver.com an "information service"

REGULATORY UNCERTAINTY (cont'd)

DOJ/FBI/DEA filed a petition for rulemaking requesting the FCC resolve a number of outstanding issues:

- Identify the types of entities that are subject to CALEA

- Establish packet-mode compliance benchmarks and deadlines

- Provide for future technology benchmarks and deadlines

- Establish procedures for enforcement

- Confirm carriers bear sole financial responsibility for post-95 equipment, facilities, and services

- Permit carriers to recover implementation costs from customers

THE PETITION HAS BEEN INACCURATELY PORTRAYED – SCOPE

Myth: the CALEA petition seeks to apply CALEA to all types of IP-based communication services

pulver.com

Skype

Microsofts' Xbox Live gaming service

E-mail service

Instant messaging, and

Visits to Web sites

Reality: Petition *proposed* coverage of broadband Internet access service providers and certain broadband telephony service providers such as Vonage

THE PETITION HAS BEEN INACCURATELY PORTRAYED – STIFLING INNOVATION

Myth: the CALEA petition would give Law Enforcement a right of prior approval over new communication services

Reality: Petition does not affect the introduction of any new service or feature

Industry continues the right to adopt CALEA technical standards, either through public standard-setting bodies or private arrangements with their respective equipment vendors
However, petition introduces accountability

THE PETITION HAS BEEN INACCURATELY PORTRAYED – BROADBAND CARRIERS

Myth: Broadband carriers are information service providers and exempt from CALEA

Reality: That legal issue remains very unsettled

FCC's express ruling that CALEA applies regardless of changes in technology

Cable Modem proceeding and Ninth Circuit decisions

Whether communications are provisioned in narrowband or broadband mode doesn't matter

THE PETITION HAS BEEN INACCURATELY PORTRAYED – EXISTING CAPABILITIES

Myth: Law enforcement has packet-mode intercept technologies of its own

Reality: Don't believe everything you see on T.V.

In many cases, the information law enforcement needs is only available with the assistance of the service provider

Law enforcement simply does not have the resources to address every technology and service

THE PETITION HAS BEEN INACCURATELY PORTRAYED – VOLUNTARY COMPLIANCE

Myth: Broadband service providers will assist law enforcement through “voluntary efforts”

Reality: Some service providers are good corporate citizens and others are not

Law enforcement cannot leave national security to the whims of corporate goodwill

Congress recognized that law enforcement assistance must be ensured through federal mandate

THE PETITION HAS BEEN INACCURATELY PORTRAYED – EXCESSIVE COSTS

Myth: the CALEA petition would impose excessive costs on industry

Reality: CALEA solution vendors have verbally advised the FBI that bringing packet-mode networks into compliance with CALEA is more cost effective and efficient than circuit-mode networks, particularly as part of an integrated enterprise solution, with security and quality of service features

THE PETITION HAS BEEN INACCURATELY PORTRAYED – PRIVACY

Myth: applying CALEA to packet-mode communications would infringe on customer privacy rights

Reality: services covered by CALEA are subject to more privacy requirements because CALEA contains built-in privacy protections

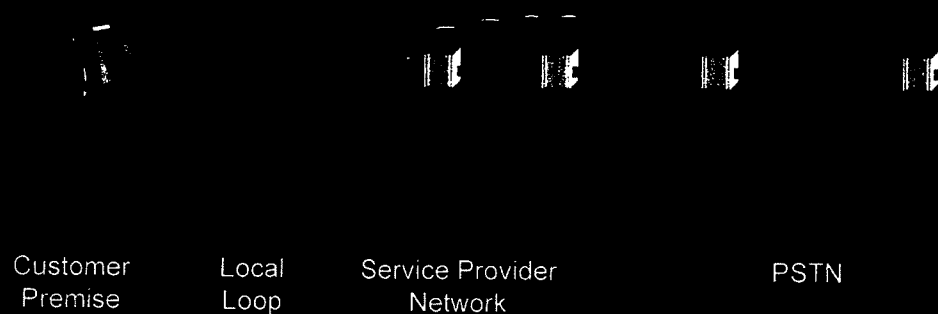
Section 105 requires providers to follow certain surveillance provisioning procedures

Section 103 requires providers to “isolate” the communications of the targeted customer

SIMPLE CIRCUIT SWITCH-BASED TRANSMISSION

Electronic surveillance was conducted in the local loop

CALEA necessitated surveillance move into the service provider network (i.e., switch-based interceptions)



PACKET-BASED ACCESS PROVIDER TRANSMISSION

The composition of a service provider's network should be transparent to law enforcement

Information available to law enforcement should be reflective of the services provided



Customer
Premise

Local
Loop

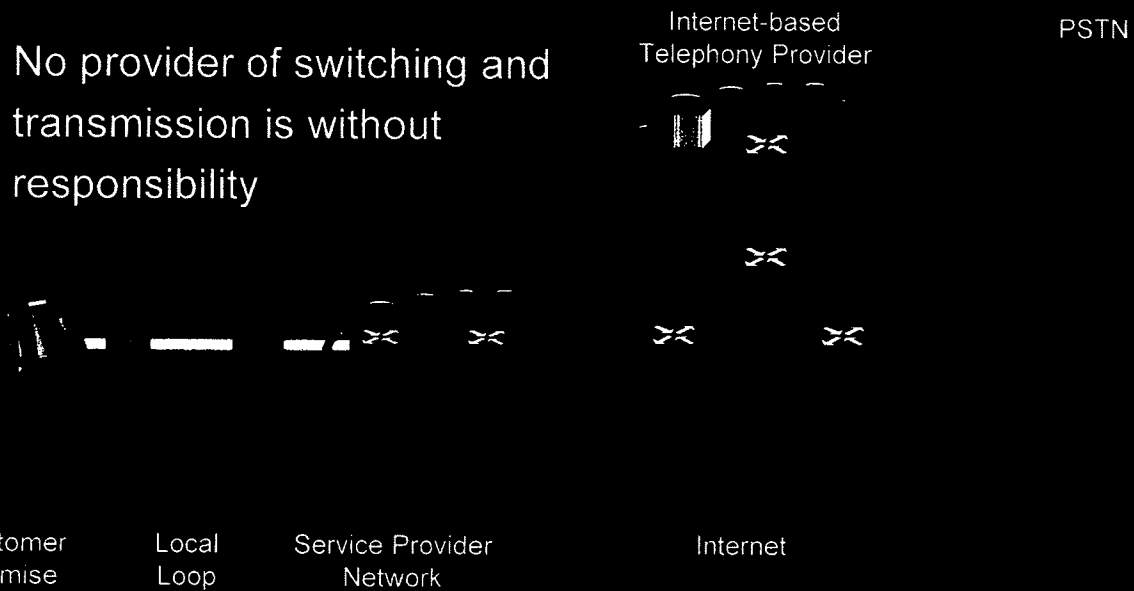
Service Provider
Network

PSTN

INTERNET-BASED TELEPHONY TRANSMISSION

Access providers are responsible for surveillance of the service they provide

No provider of switching and transmission is without responsibility



Customer
Premise

Local
Loop

Service Provider
Network

Internet

Where we go from here . . .

THE FUTURE OF ELECTRONIC SURVEILLANCE /S CALEA

Technologies and services will continue to advance –
VoIP is just the next step

Electronic surveillance must remain an effective tool

Affirmative requirements, with concrete deadlines, must
be imposed and met

The challenges of CALEA implementation will only
become more severe over time as new technologies
and services are introduced if appropriate steps are not
taken prior to service deployment

**THE COMMUNICATIONS ASSISTANCE FOR
LAW ENFORCEMENT ACT (CALEA)
AN INTRODUCTION**

**COMMUNICATIONS FRAUD CONTROL
ASSOCIATIONS (CFCA)**

October 12, 2005

CALEA BACKGROUND

CALEA was enacted in 1994 responding to 1980's technological changes that limited law enforcement's ability to conduct electronic surveillance despite having statutory authority

CALEA does not apply to a specific technology, but rather covers all forms of telecommunications and is technology-neutral

The intent of CALEA was to be forward-looking and put industry on notice with respect to future services and law enforcement's electronic surveillance needs

WHAT IS CALEA ABOUT?

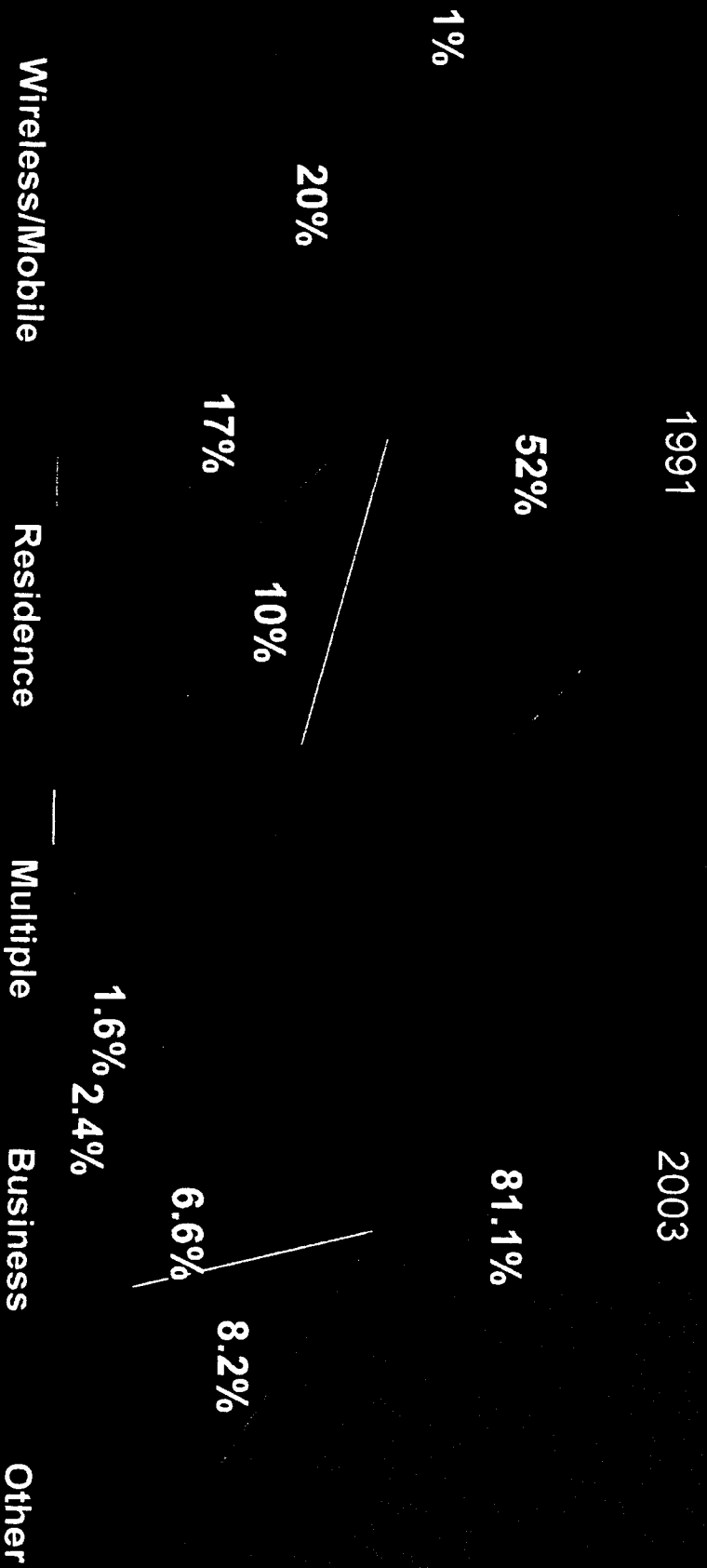
CALEA is about **ACCESS** not *AUTHORITY*

The intent of CALEA is to ensure that law enforcement has the capability to intercept all call content and call-identifying information coming from or directed to the telecommunications instrument that is the subject of a lawfully-authorized electronic surveillance

WHERE TITLE III WIRETAP AUTHORIZATIONS OCCUR

Shift in location of wiretaps

Importance of electronic surveillance of wireless / mobile

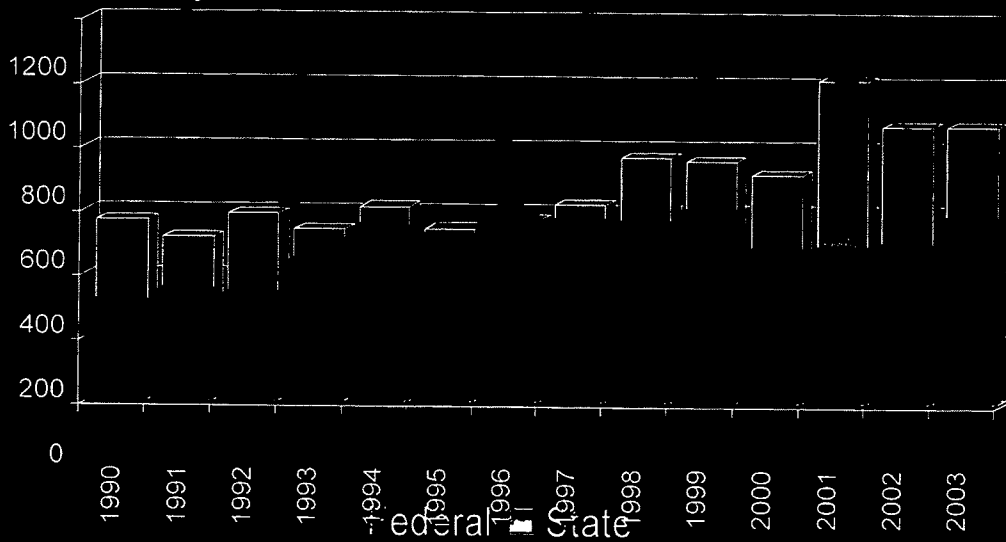


WHY THE FBI'S CALEA EFFORTS REPRESENT THE ENTIRE LAW ENFORCEMENT COMMUNITY

Title III Wiretap Authorizations 1990-2003

Only in 1996, did Federal wiretaps equal those of State and Local law enforcement (i.e., 1:1 ratio)

In 2001, State and Local law enforcement wiretaps outnumbered Federal by a 2:1 ratio

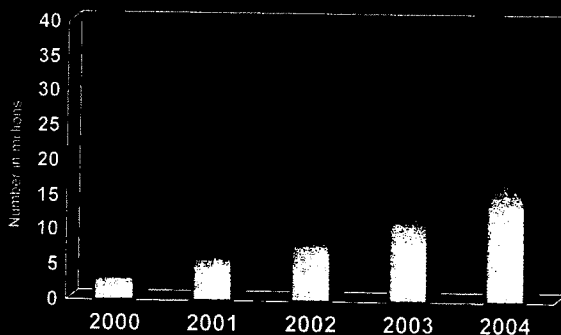


TECHNOLOGICAL CONVERGENCE IS OCCURRING AT AN UNPRECEDENTED PACE

Broadband subscribers, led by cable modem and DSL, grew from almost 19 million in 2002 to more than 37 million in 2004

Subscribers are expected to increase to more than 60 million in 2008

Law enforcement needs standardized surveillance capabilities for broadband services



FCC'S FIRST REPORT AND ORDER AND FURTHER NOTICE OF PROPOSED RULEMAKING (FNPRM)

On September 23, 2005, the FCC released a Report & Order regarding the scope of CALEA:

Facilities-based broadband Internet access providers

Providers of interconnected voice over Internet Protocol (VoIP) service

In its FNPRM, the FCC will address a number of other issues:

Compliance extensions and exemptions

Cost recovery

Identification of future services and entities subject to CALEA

Enforcement

FCC'S FIRST REPORT AND ORDER AND FNPRM (cont'd)

Report and Order based on a Joint Petition filed by
DOJ / FBI / DEA – March 10, 2004

FCC issued a Notice of Proposed Rulemaking (NPRM)
on August 9, 2004, requesting comments on a broad
range of issues

- Types of entities subject to CALEA

- Future technology benchmarks and deadlines

- Procedures for enforcement

- Consider financial responsibility for post-95 equipment, facilities,
and services

- Recover of implementation costs

FCC'S TREATMENT OF ISSUES COVERAGE OF BROADBAND ACCESS

Broadband internet access falls within CALEA's scope

Substantial Replacement Provision

Traditional telephone service was (at one time) the only means to access the Internet

Is an information service for other regulatory purposes

The FCC held in its Cable Modem Declaratory Ruling that broadband Internet access service is an information service under the Communications Act's definition

FCC'S TREATMENT OF ISSUES COVERAGE OF BROADBAND TELEPHONY

Broadband telephony falls within CALEA's scope

Same Substantial Replacement Provision logic

The FCC requested comment on the appropriateness of the distinction between managed and non-managed VoIP communications for purposes of CALEA

"Managed" or "mediated" services: the provider mediates or manages the communication and provides call set-up, connection, termination, and party identification features...

"Non-managed," or "disintermediated" services: the provider has minimal or no involvement in the flow of packets, serving instead primarily as a directory that provides users' Internet web addresses

The FCC chose to distinguish between types of broadband telephony based on whether it was "interconnected"

THE REPORT AND ORDER HAS BEEN INACCURATELY PORTRAYED – PRIVACY

Myth: applying CALEA to packet-mode communications would infringe on customer privacy rights

Reality: services covered by CALEA are subject to more privacy requirements because CALEA contains built-in privacy protections

Section 105 requires providers to follow certain surveillance provisioning procedures

Section 103 requires providers to “isolate” the communications of the targeted customer

THE REPORT AND ORDER HAS BEEN INACCURATELY PORTRAYED – SCOPE

Myth: the CALEA petition seeks to apply CALEA to all types of IP-based communication services

E-mail service, pulver.com, Skype, X-Box Live

Visits to Web sites

Reality: Report and Order identifies coverage of broadband Internet access service providers and certain broadband telephony services (i.e., interconnected with the PSTN - such as Vonage)

THE REPORT AND ORDER HAS BEEN INACCURATELY PORTRAYED – STIFLING INNOVATION

Myth: the Report and Order gives Law Enforcement a right of prior approval over new communication services

Reality: Law enforcement is statutorily prohibited from “barring” any technology or service and petition does not affect the introduction of any new service or feature

THE REPORT AND ORDER HAS BEEN INACCURATELY PORTRAYED – BROADBAND CARRIERS

Myth: Broadband carriers are information service providers and exempt from CALEA

Reality: Law enforcement believed broadband services are covered and its Petition requested the FCC end the ambiguity surrounding this issue. The Report and Order provides much needed clarity on this issue

THE REPORT AND ORDER HAS BEEN INACCURATELY PORTRAYED – VOLUNTARY COMPLIANCE

Myth: Broadband service providers assist law enforcement through “voluntary efforts” and that is enough to safeguard the capability

Reality: Some service providers are good corporate citizens and others are not

Law enforcement cannot leave national security to the whims of corporate goodwill

Congress recognized that law enforcement assistance must be ensured through federal mandate

Uniform requirements would “level the playing field”

CALEA IMPLEMENTATION HAS BEEN INACCURATELY PORTRAYED – CALEA HAS FAILED IN THE PSTN

Myth – CALEA has not worked well in the context of the public switched telephone network

Reality – In many ways, CALEA has been very successful

The majority of today's intercepts are CALEA-compliant

Over 80 percent of all intercepts are on wireless phones

Enhanced delivery capabilities have virtually eliminated the industry's capacity and cost issues

CALEA ISSUES AND LAW ENFORCEMENT'S ROLE: TECHNICAL STANDARDS

The FBI solicits the law enforcement community for specific technical capabilities

Law enforcement members review and provide input to:

- Documented law enforcement needs

 - Packet Surveillance Fundamental Needs (PSFN)

 - Carrier-Grade Voice over Packet (CGVoP)

 - Public Internet Protocol Network Access Services (PIPNAS)

- Resulting technical contributions into industry's standards process

DOMESTIC STANDARDS ORGANIZATIONS

Voice Services Over Cable
Television Networks

CALEA General Oversight
Wireline, Wireless,
Broadband PCS

CDMA2000 Wireless Intersystem
Technology and Multimedia Services

CDMA2000 Adjunct Wireless
Packet Data Technology

Satellite Equipment
and Systems

GSM Technology Voice,
Multimedia, Packet Data

Wireline Voice over
IP, ATM and MPLS

OAM&P for Surveillance
Capabilities

GSM Global System for Mobile
PCS Personal Communications Services
CDMA2000 Code Division Multiple Access 2000
OAM&P Operations, Administration, Maintenance & Provisioning

ATM Asynchronous Transfer Mode
IP Internet Protocol
MPLS Multi Protocol Label Switching

INTERNATIONAL STANDARDS ORGANIZATIONS

General Oversight

LI for IP Traffic

LI for Softswitch-based
Networks

LI for GSM UMTS
Systems (includes
GPRS)

IP Internet Protocol
GSM Global System for Mobile
UMTS Universal Mobile Telecommunication System
GPRS General Packet Radio Service
LI Legal Intercept

CALEA CAREFULLY AND THOUGHTFULLY BALANCES THREE IMPORTANT INTERESTS

Law enforcement's legitimate needs

Industry's concerns about the potential burden

Important privacy concerns

QUESTIONS?

[REDACTED] Acting Unit Chief
CALEA Implementation Unit
Federal Bureau of Investigation

b6
b7c

[REDACTED]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 11-24-2008 BY 60322/UCLRP/PJ/EHL

Technical and Legal Challenges With Intercepting Emerging Technologies

 Unit Chief

CALEA Implementation Unit (CIU)

July 2007

b6
b7c



AGENDA

b2
b7E

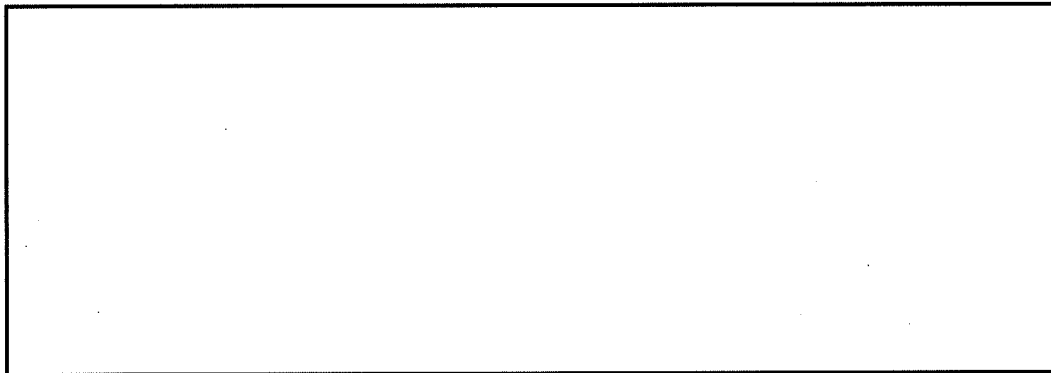
- **Technical Challenges Presented by Emerging Technologies**
- **Migration in Wireless Handset Capabilities**
- **Technical Challenges with**
- **Legal Challenges Presented with**



INTERCEPTION CHALLENGES RESULTING FROM EMERGING PACKET-BASED COMMUNICATION SERVICES

b2
b7E

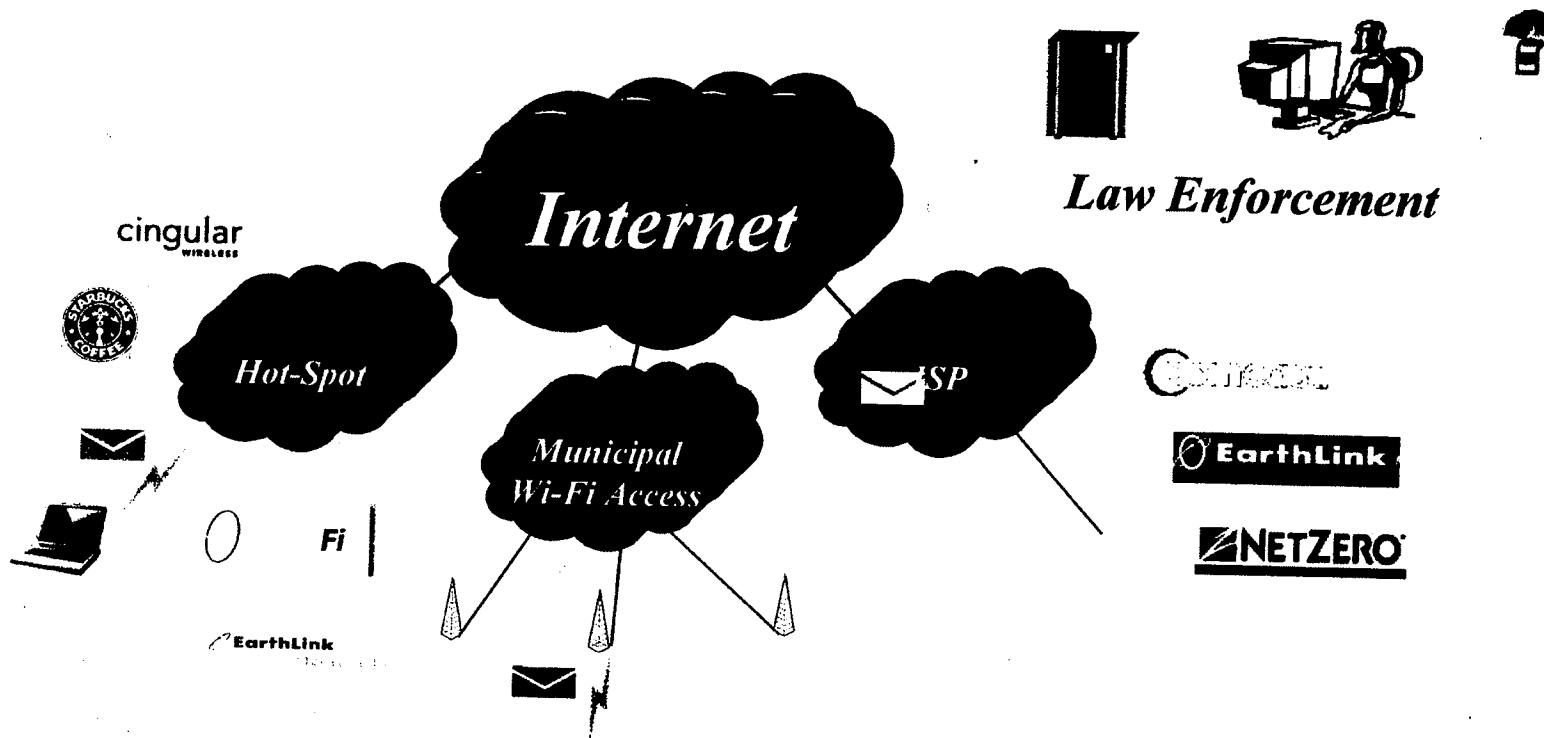
- **Packet-based services are evolving to offer new features and capabilities to subscribers which were not available on traditional telecommunication networks**
- **This evolution presents several challenges to law enforcement, including**





TARGET MOBILITY

b2
b7E

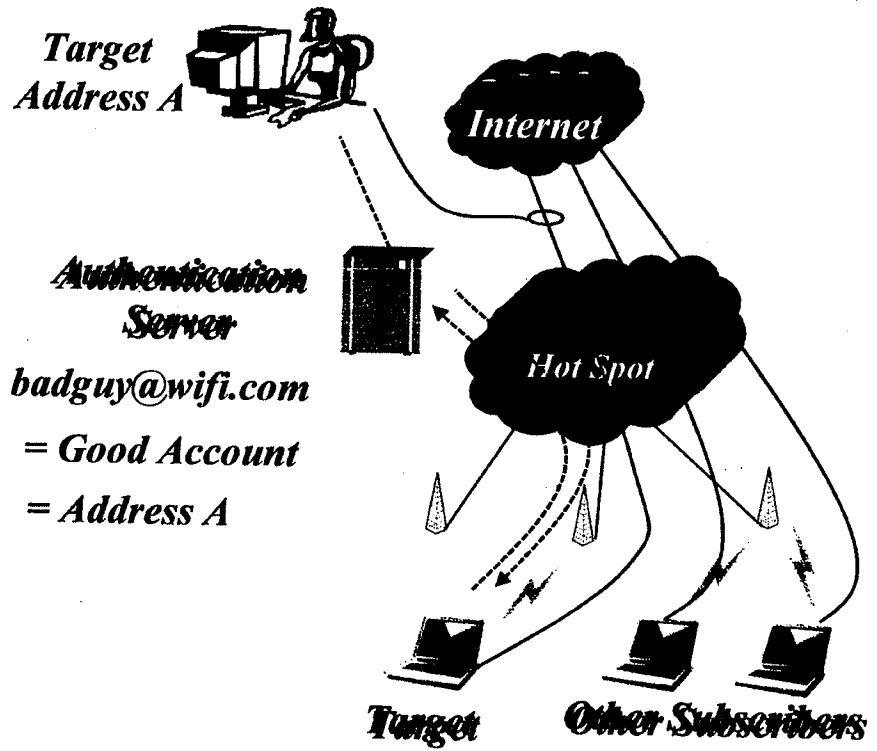


- **A subscriber may roam from location to location without impacting their services**
- [Redacted]

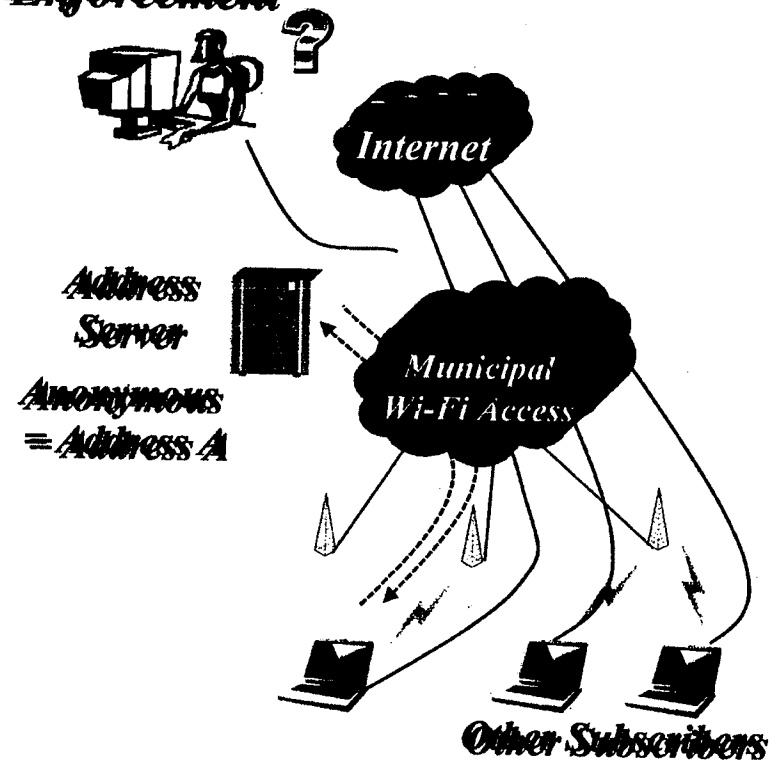


TARGET IDENTIFICATION

Law Enforcement

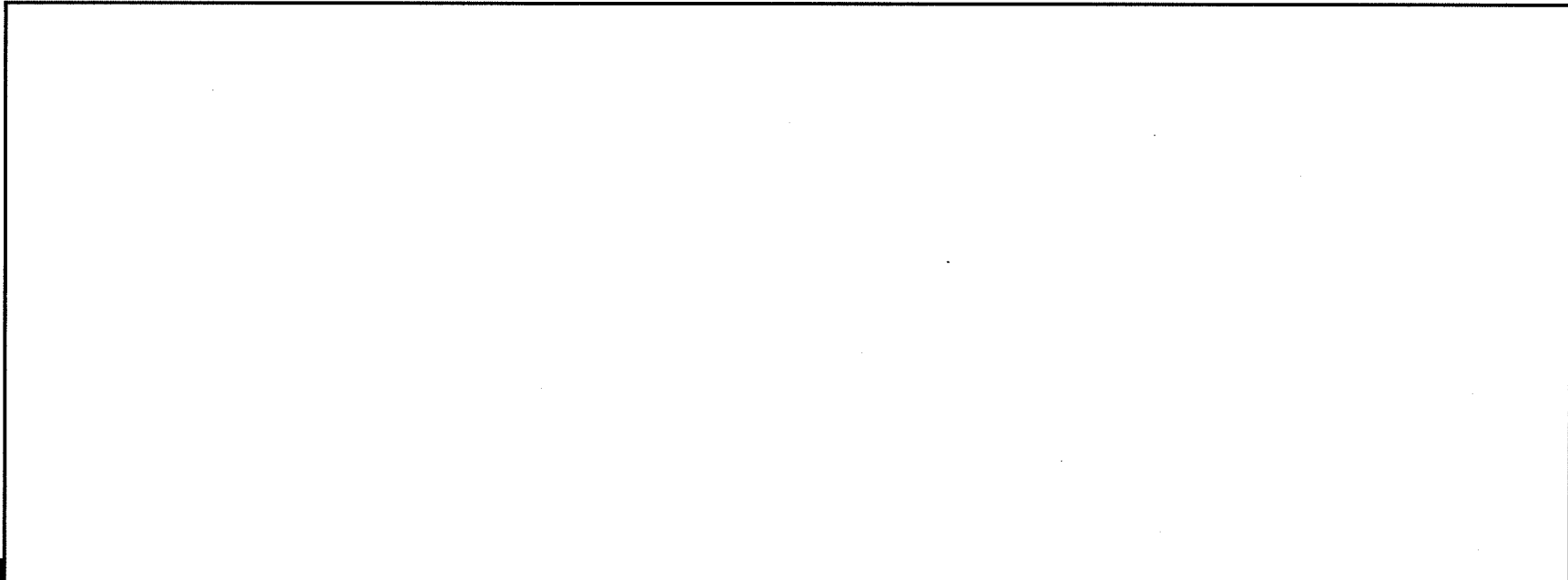
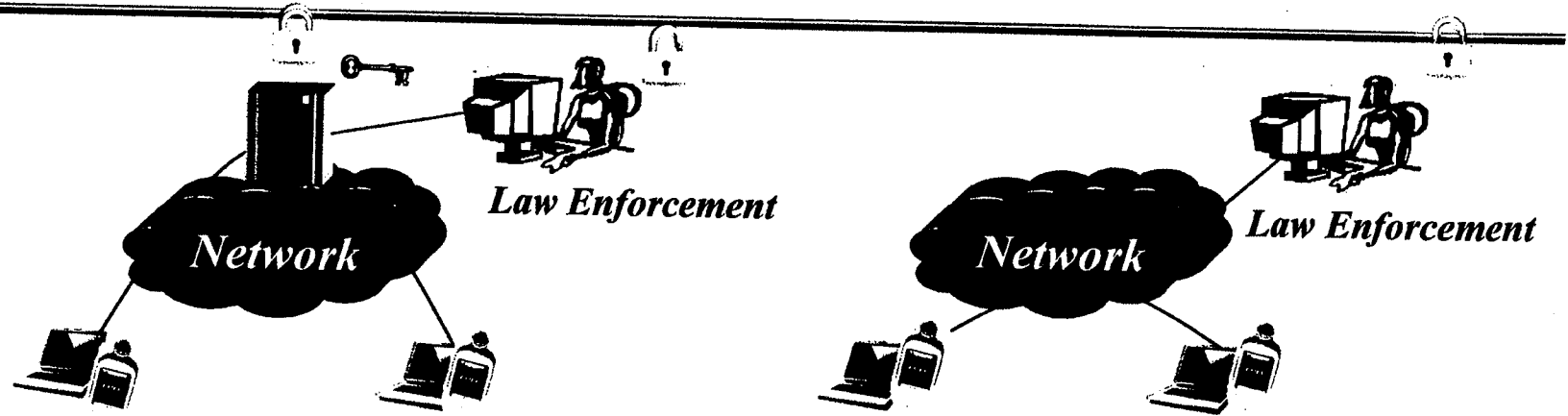


Law Enforcement





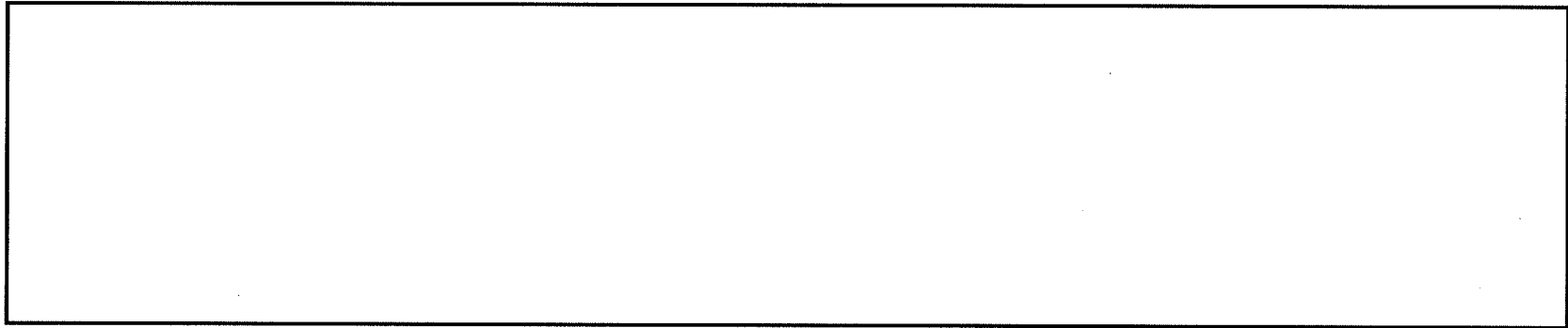
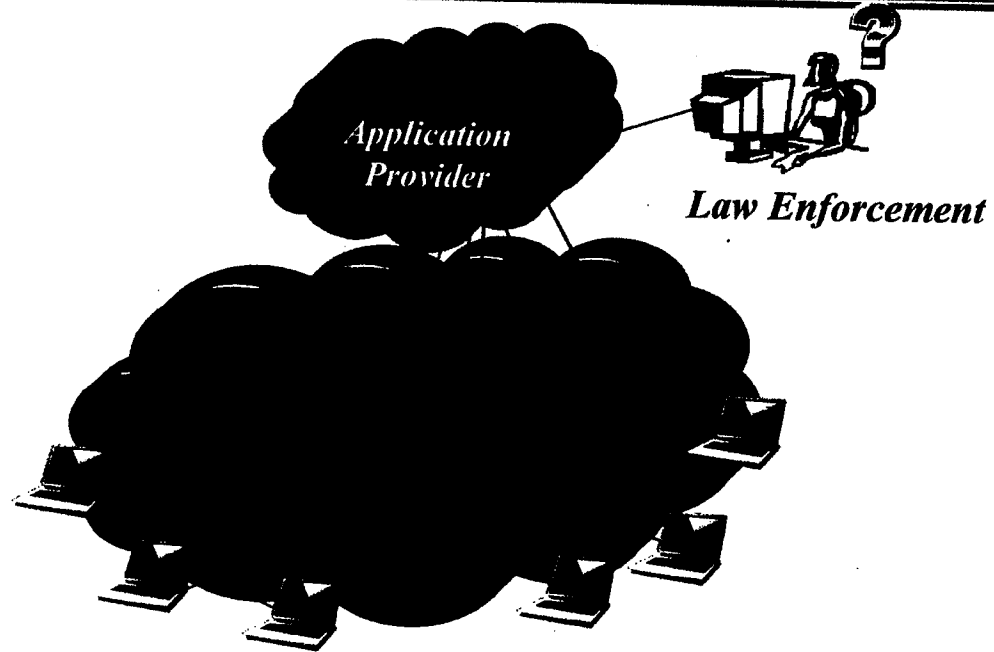
ENCRYPTION





PEER-TO-PEER

b2
b7E

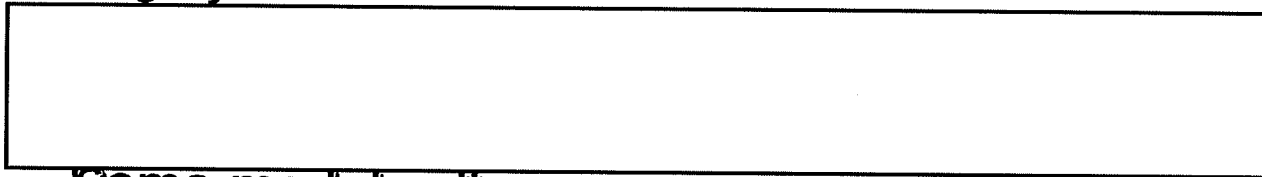




CELLULAR COMMUNICATION SERVICES – THE “PERFECT STORM” OF CHALLENGES

- **Modern smart phones combine the mobility of traditional cell phones with the capabilities of fixed computers**

- *Highly mobile*



- *Some models allow seamless switching between networks for voice and data services*

- **Will become more popular with the average consumer as costs are reduced and their interfaces become more accessible (e.g., Apple’s iPhone)**



ALWAYS ON, ALWAYS CONNECTED, ALWAYS MOVING WIRELESS SERVICES / CAPABILITIES



- 2.5G (GPRS)
- 3G (UMTS)
- Wi-Fi
- Bluetooth
- GPS
- 3rd Party Applications
- Keyboard
- Touch Screen
- Price (with contract)

iPhone



Cingular 8525



Blackberry Curve



Samsung Blackjack



\$499.99

\$299.99

\$199.99

\$99.99

T Mobile

Blackberry 8800



Sidekick



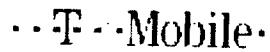
Blackberry Pearl



Dash



2.5G (GPRS)				
3G (UMTS)				T
Wi-Fi				
Bluetooth	T	T	T	T
GPS				
3rd Party Applications	T	T	T	T
Camera				
Keyboard	T	T	T	T
Touch Screen				
Price (with contract)	\$349.99	\$199.99	\$149.99	\$149.99

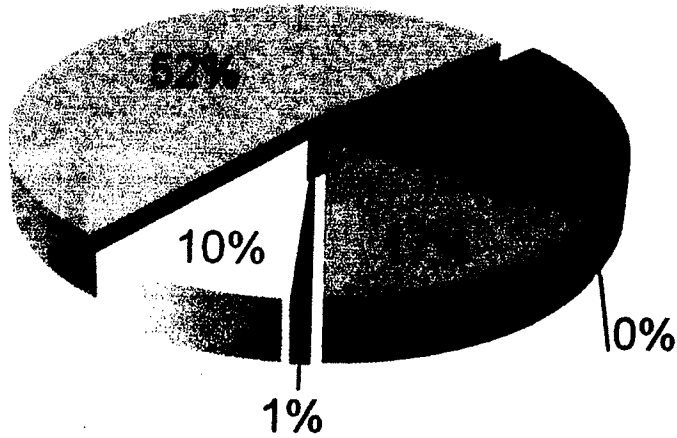




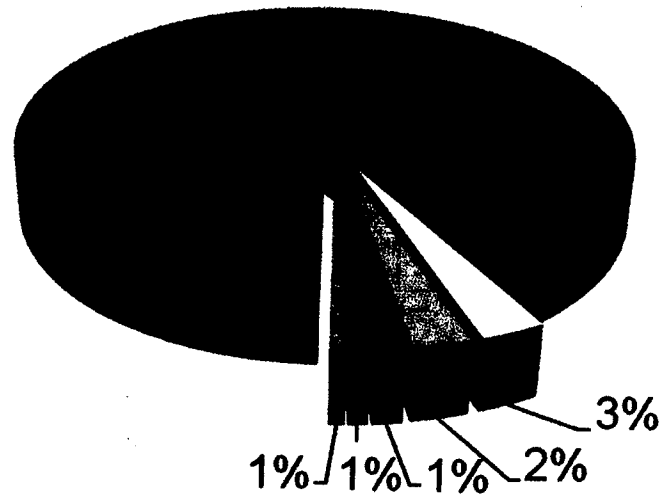
ELECTRONIC SURVEILLANC TRENDS - WHERE TITLE III WIRETAP AUTHORIZATIONS OCCUR

- **Shift in location of wiretaps**
- **Wireless / mobile technologies are the preferred medium of communications for targets**

1991



2006

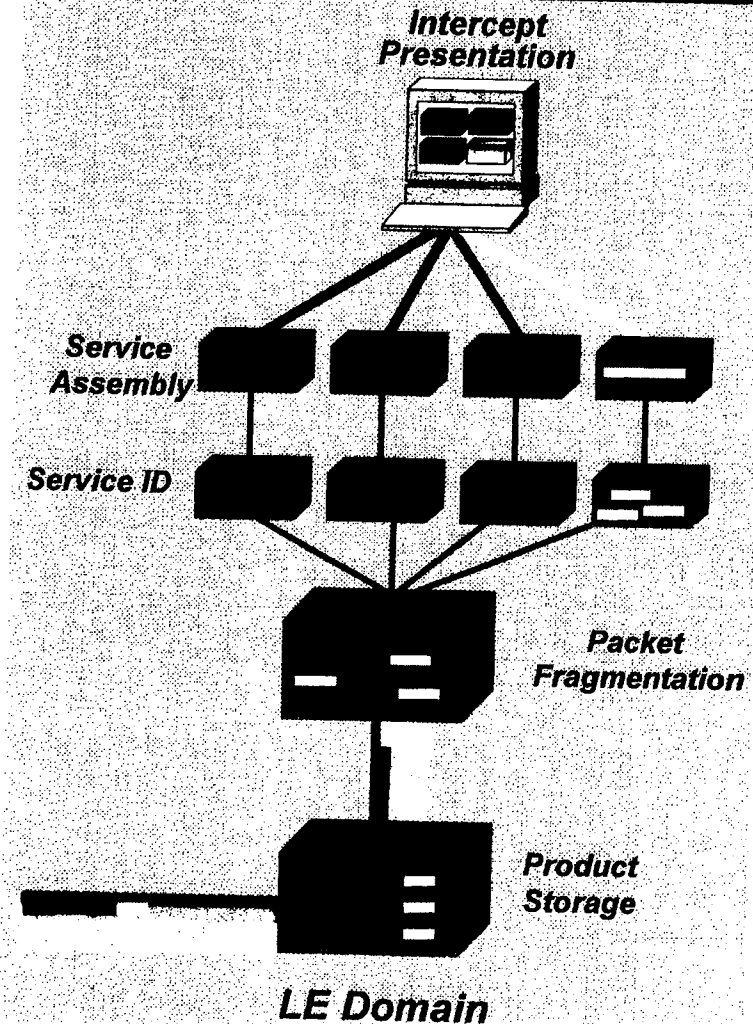


Wireless/Mobile
 Residence
 Multiple
 Business
 Roving
 Other



PROCESSING AND VIEWING COLLECTED DATA

- Once isolated, Law enforcement must process the individual applications
 - Collection equipment is more costly with no commercially available products which meet operational needs
 - Requires law enforcement training on application level processing and analysis
 - Application providers continually change and modify their services, requiring updates to the law enforcement collection equipment
- Impacts of the volume of data collected
 - Broadband interception requires significant storage
 - Significant LE resources are required to analyze all the collected data





TECHNICAL CHALLENGES WITH PROTOCOL PROCESSING AND APPLICATION COMPLEXITY

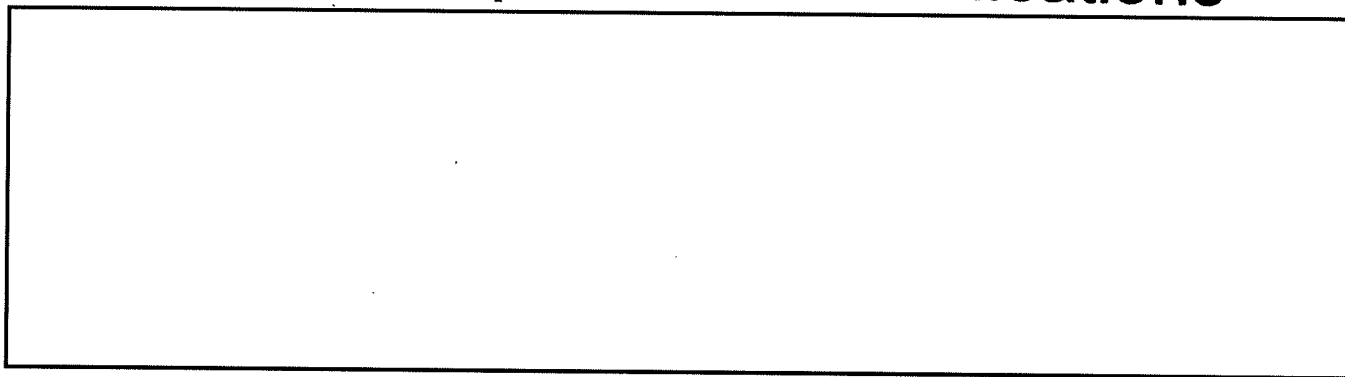
- **Implementations of packet-based services no longer rely on standardized architectures and protocols**
 - Many packet-based services are built upon non-standardized or proprietary offerings
 - Both the protocols and architecture may be implemented in a provider-specific manner
 - Creates an environment of significant possibility for variations in implementation
 - Providers continually update and modify their applications to be more competitive
 - Information available in one network may not be available in another



b2
b7E

CHALLENGES WITH TITLE III INTERCEPTION OF EMERGING TECHNOLOGIES

- **The combination of several technical factors present unique legal challenges with the interception of packet communications**





TITLE III COVERAGE: KEY DEFINITIONS

- **“intercept”** - acquiring contents of a communication using a device
- **“contents”** - substance purport or meaning of a communication
- **“wire communication”** -
 - involving the human voice
 - at least partly through use of a wire
 - includes through a “switching station”
 - includes “electronic storage” of a communication

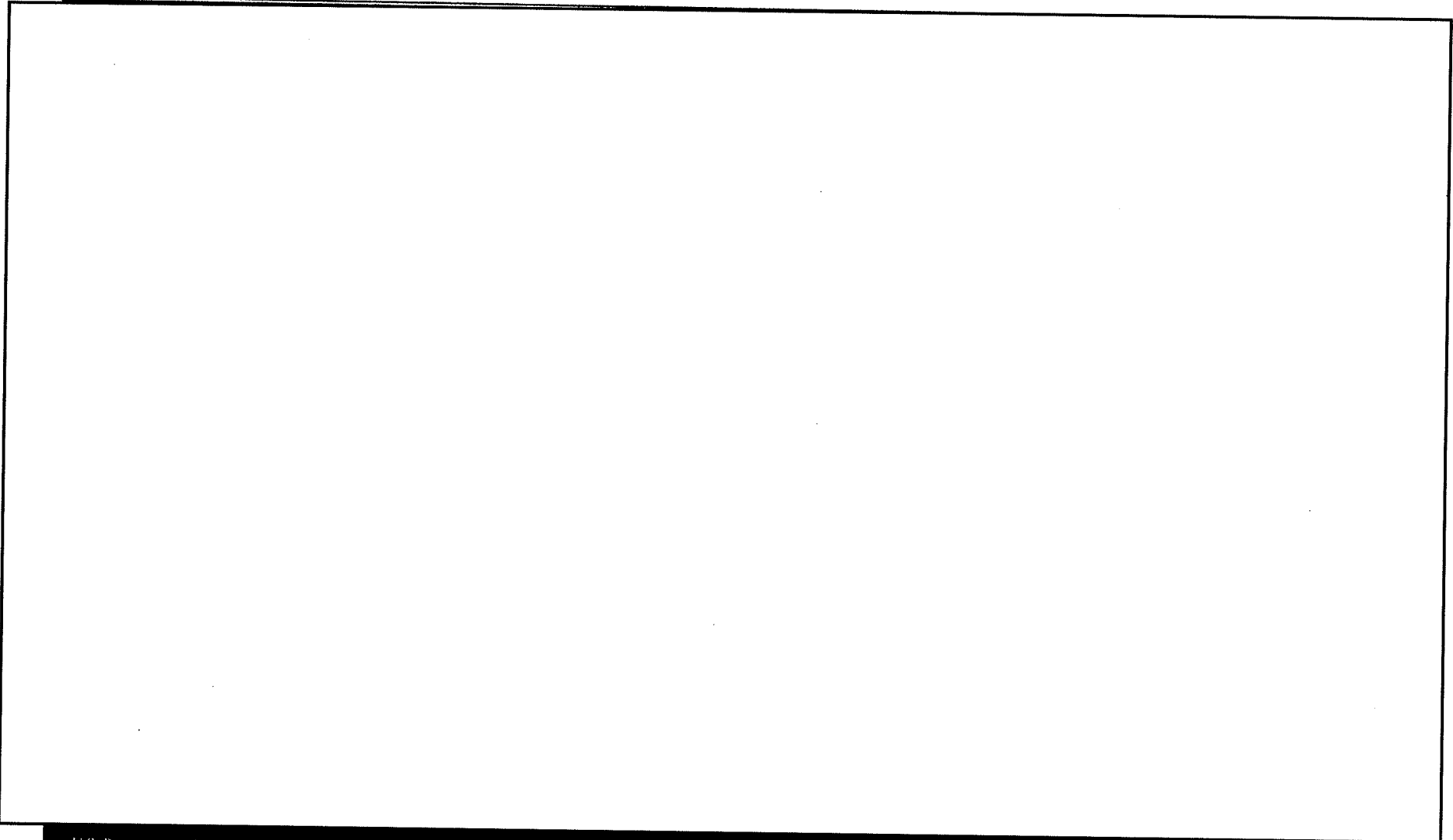


TITLE III COVERAGE: KEY DEFINITIONS

- **“electronic communication” - any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature, transmitted in whole or in part by wire, radio, electromagnetic, photoelectronic, or photooptical system except:**
 - a wire or oral communication
 - tone only paging device
 - tracking device
 - electronic funds transfer



CHALLENGES IDENTIFYING WIRE AND ELECTRONIC COMMUNICATIONS IN PACKET NETWORKS

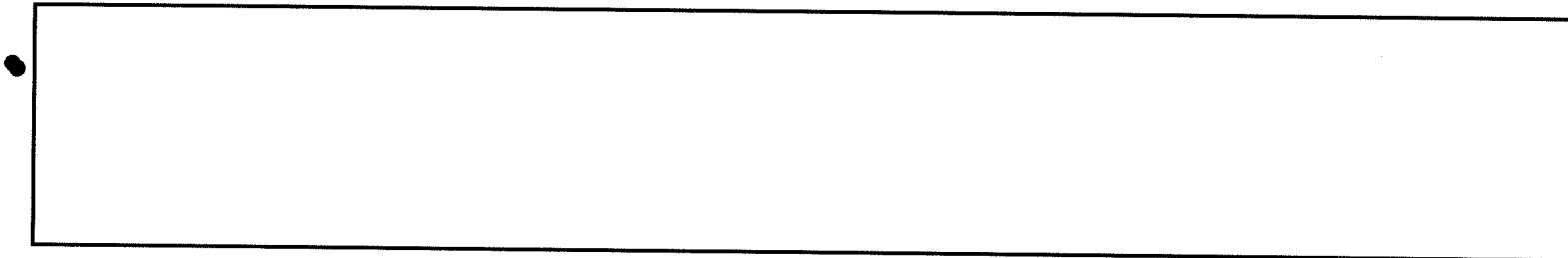




SUMMARY

b2
b7E

- **Emerging technologies present a unique set of technical challenges to law enforcement's ability to conduct electronic surveillance**
- **Cellular communications are becoming more sophisticated, offering all of the capabilities previously associated with fixed broadband services in a mobile, light weight device**





QUESTIONS