U.S. CALEA Market Insight

6841-63

Frost & Sullivan takes no responsibility for any incorrect information supplied to us by manufacturers or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation.

Frost & Sullivan reports are limited publications containing valuable market information provided to a select group of customers in response to orders. Our customers acknowledge when ordering that Frost & Sullivan reports are for our customers' internal use and not for general publication or disclosure to third parties.

For information regarding permission, write:

Frost & Sullivan
2400 Gerg Road, Suite 201
Palo Alto, CA 94303-3331
United States

Table of Contents

Chapter 1

U.S. CALEA Market

Executive Summary 1-1

CALEA Market Introduction 1-1

Brief CALEA Overview 1-2

Highlights of the CALEA Study 1-3

Frost & Sullivan Awards 1-5

Frost & Sullivan Award: CALEA Market Leader Award 1-5

Award Category: CALEA Market Leadership Award 1-5

Award Description 1-6

Research Methodology 1-6

Measurement Criteria 1-7

Frost & Sullivan Award: CALEA Technology Innovation Award 1-7

Award Description 1-9

Research Methodology 1-9

Measurement Criteria 1-9

State of the CALEA Market 1-9

Market Engineering Measurements—Snapshot of the CALEA Market 1-9

History of CALEA 1-11

Background of the Act 1-11

Wiretapping History 1-11

The "Punch List" and Legal Requirements 1-15

The "PUNCH LIST" 1-16

Types of Surveillance 1-17

CALEA Funding and Resources 1-18

CALEA Funding and Associated Costs 1-18

Wiretapping Facts and Figures 1-22

Wiretapping Expenditures in the U.S. 1-25

CALEA Technical Analysis 1-26

Basic CALEA Analysis (TDM & PSTN) 1-26

The Court Order Process 1-28

Wireless Analysis 1-28

Packet & IP-Based Analysis 1-29

Future of IP and CALEA 1-31

Architecture of Wireless IP 1-32

Resources and Definitions 1-33

Acronyms and Definitions 1-33

CALEA Associations and Organizations 1-34

CALEA Compliancy Organizations 1-34

Organizations and Associations 1-34

The Standards 1-34

Other Resources 1-34

List of Figures

Chapter 1

U.S. CALEA Market

1-2 Government and Service Provider Obligations for Wiretapping Legislation, 1791-2001 1-13

1-4 Wiretap Statistics for 2001 and 2002 1-19

1-5 Wiretap Application Statistics by State for 2002 1-19

1-6 Telecommunications Carrier Compliance Funding: FY 1997-2001 1-21

List of Charts

Chapter 1

U.S. CALEA Market

1.1 CALEA Telecommunications Market: Market Engineering Measurements (U.S.), 2002 1-10

1.2 U.S. CALEA Market: History of Legal Acts, 2003 1-12

1-1 Legislation, Proponent and Reasoning for Wiretapping Legislation, 1791-2001 1-12

1.3 Federal Title III Wiretaps, 1968-1998 1-17

1-3 CALEA Compliance Funding: Fiscal Years 1997-2001 1-18

1.4 Wiretaps by Location, 2001 1-22

1.5 CALEA Wiretaps by Medium, 2001 1-23

1.6 Wiretaps for Electronic Devices by Segment for 2001 1-23

1.7 Wiretaps for Electronic Devices by Segment for 2001 1-24

1.8 2001 Wiretaps by Type of Criminal Investigaticon 1-24

1.9 Governmental Spending on Wiretaps for 2000 and 2001 by Segment 1-25

1.10 Forecast of Total U.S. Wiretap Spending, 2002-2007 1-25

1.11 Forecast of CALEA Wiretaps for both U.S. Federal and State Agencies, 2001-2007 1-26

1.12 PSTN CALEA Architecture Diagram 1-27

1.13 IP Network CALEA Architecture Diagram 1-29

1.14 Mobile IP CALEA Network 1-32

1

U.S. CALEA Market

Executive Summary

CALEA Market Introduction

Telecom carriers across the world are dealing with the pressing issue of CALEA compliance that directly affects telecommunications infrastructure, provisioning, and signaling services. The Communications Assistance for Law Enforcement Act was implemented in 1994 to preserve the ability of law enforcement agencies (LEAs) to conduct electronic surveillance in the face of rapid advances in telecommunications technology. Carriers must meet requirements to assist LEAs with the wiretapping and intercept process.

Because the nation's communications networks are routinely used in the commission of serious criminal activities, including espionage, wiretapping is performed for evidence collection. Organized crime groups and drug trafficking organizations rely heavily upon telecommunications to plan and execute their criminal activities. The ability of law enforcement agencies to conduct lawful electronic surveillance of the communications of its criminal subjects represents one of the most important capabilities for acquiring evidence to prevent serious criminal behavior. Unlike evidence that can be subject to being discredited or impeached through allegations of misunderstanding or bias, electronic surveillance evidence provides jurors an opportunity to determine factual issues based upon a defendant's own words.

Under Title III, applications for interception require the authorization of a high-level Department of Justice (DOJ) official before the local United States Attorney's offices can apply for such orders. Interception orders must be filed with federal district court judges or before other courts of competent jurisdiction. Hence, unlike typical search warrants, federal magistrates are not authorized to approve such applications and orders. Further, interception of communications is limited to certain specified federal felony offenses. The majority of approved intercepts are performed at the state jurisdiction levels, as compared to federal levels. The majority of the most recent intercepts are also being performed over wireless voice and data mediums.

Applications for electronic surveillance must demonstrate probable cause and state with particularity and specificity: the offense(s) being committed, the telecommunications facility or place from which the subject's communications are to be intercepted, a description of the types of conversations to be intercepted, and the identities of the persons committing the offenses that are anticipated to be intercepted. Thus, criminal electronic surveillance laws focus on gathering hard evidence—not intelligence.

Applications must indicate that other normal investigative techniques will not work or are too dangerous, and must include information concerning any prior electronic surveillance regarding the subject or facility in question. Court orders are limited to 30 days and longer with approved extensions, and interceptions must terminate sooner if the objectives are obtained. Judges may (and usually do) require periodic reports to the court (typically every 7-10 days) advising it of the progress of the interception effort. This circumstance thus assures close and ongoing oversight of the electronic surveillance by the United States Attorney's office handling the case. Extensions of the order (consistent with requirements of the initial application) are permitted, if justified, for up to a period of 30 days.

Electronic surveillance has been extremely effective in securing the conviction of more than 25,600 dangerous felons over the past 13 years. In many cases there is no substitute for electronic surveillance, as the evidence cannot be obtained through other traditional investigative techniques. There are however public privacy issues and concerns because of the wiretapping process which may infringe on the listening of private and confidential conversations. With packet-based communication delineating the header packet from the call identifying packet can present even more problems with protection of individual privacy.

Brief CALEA Overview

Communications Assistance for Law Enforcement Act, or CALEA was passed in 1994 in order to help the U.S. government foster interaction with communications carriers to make wiretapping easier. This interaction was necessary due to the growth in new types of communications, like wireless phones and email, along with rapid advances in technology. CALEA has been relatively successful; carriers have never been fined for non-compliance, something that is stipulated in the law for being uncooperative.

After CALEA was passed, Congress allocated $500 million to subsidize the cost of implementing new switches in the telecommunications networks of the U.S. carriers, with most of that money already spent. Government agencies spend around $70 million annually on wiretaps, with an estimated $50,000 in costs per wiretap. This is a very small market for telecommunications services, and it is not a profitable endeavor for carriers. Carriers may spend between 50,000 and 500,000 per switch for hardware and software upgrades to become CALEA compliant.

CALEA requires carriers to isolate, enable, identify, intercept, and deliver all wire and electronic communications as required by lawful authorization. Carriers are responsible for consulting with manufacturers of their transmission and switching equipment to ensure that current and planned equipment comply with CALEA requirements. Carriers need to be able to intercept digital communications of all types. Carriers must also be capable of collecting all call identifying information including origination, direction, destination, and termination. Finally, carriers need to be prepared for next generation communication wiretapping, including electronic messaging software, information services, and telecom support. While there are ambiguous definitions as to what "information services" are, Frost & Sullivan expects CALEA compliancy requirements for most forms of communications because of the growing emphasis on homeland security and the fight against terrorism.

CALEA wiretaps can be segmented into three major functional domains: access, delivery, and collection. The access function is performed at the switch, which records the call record information, and depends on the switching vendor and also the type of transmission protocol. The delivery function is responsible for carrying the lawful intercept to the collection point. The delivery function is based on whether the call is delivered over IP or PSTN, and usually includes servers, mediation devices, routers, and other equipment that collect the call information and data. The collection function houses the LEA (Law Enforcement Agency) computer system, software, and database system. Carriers are only responsible for the access and delivery functions.

The future of government surveillance of its citizens will be based on the original CALEA act and will impact all new communications mediums and technologies. As telecommunications carriers look to VoIP to offer new services and reduce cost, wiretapping applications will be necessary. VoIP wiretapping products are in the initial phases of development; this effort currently lacks a strong financial push due to a lack of market for these solutions. Carnivore, the FBI’s Internet packet sniffing software is another relatively new development in wiretapping. It allows the FBI to monitor data sent and received by individuals; it has sparked a flurry of legal debates about privacy, but was authorized by CALEA.

Highlights of the CALEA Study

CALEA continues to be an important issue for carrier networks because of the integration and convergence of multiple communications technologies such as wireless, IP, cable, the Internet, and others.

Frost & Sullivan has identified the following important take-aways from this CALEA research service:

- There are a number of solutions available for CALEA compliancy including switch vendor solutions, adjunct solutions, service bureau solutions.
- Convergent communications and next-generation technologies stem the current and future requirements to perform lawful intercepts over cable, packet, wireless data, and eventually information services.
- The FBI CIS has a program to assist carriers in becoming CALEA compliant and adhering the six "Punch List" items.
- The FCC regulates carrier compliancy, carriers can file for extensions to prolong compliancy and prepare networks.
- Standard bodies include the Telecommunications Industry Association, Cable Labs, International Softswitch Consortium, and others (See Resources section).
- Carriers must comply with lawful intercept, which may require provisioning staff, call event management, call content and data delivery, and dedicated communications links to the Law Enforcement Agencies.
- Carriers are only responsible for the access and delivery functions of the CALEA call collection and identifying process.
- For now carriers include wireline, wireless, cable, and any other carrier providing telecom services. The definition of "Information services" remains unclear for now. Some information service are excluded from CALEA for now, but Frost & Sullivan expects Internet services and communications to eventually be required to be compliant under CALEA.
- The majority of wiretaps are performed over wireless mediums. The majority of wiretap targets are being investigated for drug trafficking and drug-related criminal behavior.
- FBI provided CALEA funding is exhausted for now. Carriers incur costs of routing, mediation, collection, equipment, transmission, security, and administration of lawful intercepts.
- The average wiretap costs the government (Federal, state, and local) over $54,000 per wiretap according to 2002 figures.
- The balancing of public safety and securing the homeland while dealing with issues of consumer and individual privacy, continue to be an issue CALEA vendors and carriers must be aware of when evaluating CALEA solutions and services.

Frost & Sullivan Award: CALEA Market Leader Award

Award Category: CALEA Market Leadership Award

Frost & Sullivan is honored to announce VeriSign Inc. as the 2003 recipient of the CALEA Market Leadership Award for their NetDiscovery Service, an innovative and cost-effective carrier solution for CALEA compliance. VeriSign's NetDiscovery service is an attractive service bureau solution, which provides carriers with a streamlined approach to the CALEA access and delivery requirements set forth by the Communications Assistance for Law Enforcement Act of 1994. This single source turnkey solution allows carriers to focus on their core business, while VeriSign acts as the mediator between the carrier and the law enforcement agency (LEA).

VeriSign released its first version of the NetDiscovery service in the summer of 2002 for wireline, wireless, and cable service providers, and in the 1st and 2nd quarter of this year released its new version, which handles wireless data and VoIP intercepts. The NetDiscovery service allows carriers to bypass the expensive operational and capital expenditures of compliance, and hand-off administration and performance of the access and delivery function to VeriSign's security administration bureau. VeriSign's security administration bureau maintains tremendous skills and knowledge of various security solutions including electronic surveillance and digital certificate technology, all running over a trusted nationwide signaling network.

While CALEA compliance is an important issue for homeland security and to assist in capturing criminals, the facilities, infrastructure, and administrative costs are prohibiting implementation. The costs of upgrading hardware and software within a carriers' switch to maybe perform zero to few wiretaps a year is a very difficult cost for carriers to justify. Carriers are currently facing CALEA costs between $50,000 up to $500,000 per switch to become CALEA compliant and to adhere to the six mandated "Punch List" items. VeriSign works closely with the FBI CIS, the FCC, numerous LEAs, and a number of CALEA standard bodies and organizations to remain proactive and educated on the latest legal, operational, and technical CALEA requirements.

Wireline, wireless, and cable service providers are burdened with the expensive and process-intensive task of complying with CALEA requirements in an effort to assist local, state, and federal law enforcement with lawful intercept (LI) or electronic surveillance. Wiretapping, including "pen register", "trap and trace", and "Title III" are all areas in which a carrier must understand and provide assistance to the LEA. The NetDiscovery service, allows carriers to perform lawfully authorized electronic surveillance (LAES), at a fraction of the

cost, and at a huge savings compared to in-house implementations. The NetDiscovery service currently provides intercept assistance with the following technologies:

- Wireline and wireless voice
- Wireline and wireless data
- Voice over IP
- Packet data services

VeriSign also continues to work with switch vendors, mediation vendors, CALEA hardware/ software vendors, carriers etc. to remain on the forefront of future CALEA requirements and compliancy issues. Current and future trials and continued expansion in the NetDiscovery service offering are opening the door to future growth in cable voice/data services, IP-based services, information services, and other next-generation communications. VeriSign's NetDiscovery Service, powered by Verint Systems Inc.'s STAR-GATE system, is truly a remarkable offer in this convergent world of communications. Frost & Sullivan would like to congratulate VeriSign for remaining a market leader in CALEA compliant solutions, and for their continued drive in providing solutions for the ever-changing communications market.

Award Description

The Frost & Sullivan CALEA Market Leadership Award is given to the company that has exhibited market leadership through the implementation of market engineering strategy, technology innovation, and unique solutions to meet the diverse needs of multiple communications networks. The recipient has displayed excellence in all areas of the market engineering process, including the identification of market challenges, drivers and restraints, as well as strategy development and methods of addressing these market dynamics. Furthermore, the award recipient has continually demonstrated solutions for monitoring market changes and for implementing superior market engineering strategies. By utilizing these strategies for success, the company has established itself as the market leader in providing carriers with a CALEA compliant solution.

Research Methodology

To choose the recipient of this award, the analysts track and evaluate competitor products/ services and solutions for CALEA compliancy. This is achieved through interviews with multiple market participants and extensive secondary research of proprietary data sources. Finally, the competitors and their respective product offerings/solutions are compared and ranked for relative position. Frost & Sullivan then presents the award to the company that received the number one industry rank.

Measurement Criteria

In addition to the methodology described above, there are specific criteria used to ascertain final competitor ranking in this industry. The recipient has excelled by substantially increasing one or more of the following criteria:

- Market leadership while meeting end-user demand
- Technology and network diversity
- Partnerships and Alliances to advance solution/service
- Architecture and technology innovation
- Attractive and in-demand solution/offering
- Flexible and efficient product/service
- Flexible customer options and on-demand service

Frost & Sullivan Award: CALEA Technology Innovation Award

Frost & Sullivan is proud to announce SS8 Networks as the CALEA Technology Innovation Award recipient for the Xcipio (TM) product line, a lawful intercept solution designed to handle the provisioning, access, delivery, and collection functions for lawfully authorized electronic surveillance. SS8 Networks first deployed lawful intercept solutions in 1994, and released the Xcipio product, a unified international platform in 2001. With over 200 deployments for both wireline and wireless carriers in the U.S., their expertise and superior knowledge of the CALEA compliant market has advanced SS8 to be a leader and innovator in lawful intercept solutions. The Communications Assistance for Law Enforcement Act of 1994 continues to be a pressing issue, and for newer technologies such as wireless, cable voice, and IP, compliance requirements are just around the corner.

The Xcipio product handles lawful interceptions for a number of different communications technologies including:

- Voice (J-STD-025 and ETSI standards)
- ISP Services (Email, Internet, Chat, IP Data)
- VoIP (PacketCable)
- Wireless Data (CDMA & GPRS)

The Xcipio product houses a number of applications to meet the needs of the traditional and next-generation communications systems and technologies. Applications such as a circuit-switch delivery function, softswitch delivery function, call data distribution function, Internet access delivery function, and collection function, address the varying needs of multiple network requirements. Four important service layer modules work to perform the full CALEA requirements including the provisioning element, the intercept engine, content processing, and a demodulation/recording module for the law enforcement agency (LEA) collection process.

SS8 Networks has over nine years of lawful intercept experience and offers an end-to-end state of the art intercept system. For carriers that require an in-house solution and prefer to perform the provisioning and control of lawful intercepts internally, SS8 offers a cost-efficient solution that is scalable to a carriers' personal network and architecture needs. Because Xcipio is an open-architecture platform, it is designed to interface with multiple switching, provisioning, and OSS systems. This also allows for easier management and timely updates for new CALEA requirements and standards.

SS8 Networks is also an important member of many CALEA and lawful intercept organizations and working groups including the International Softswitch Consortium, PacketCable, ETSI standards, TIIT (Netherlands) standards, Telecommunications Industry Association, and T1P1(3GPP). These organizations and working groups provide SS8 with valuable insight and direct input into international lawful intercept standards. Being involved in the standards organizations also gives SS8 leverage to make progressive decisions in improving electronic surveillance technologies.

SS8 Networks partners with a number of technology vendors to advance the Xcipio product. Partners include Fiducianet (Service Provider partner), BearingPoint, IBM, JSI, TopLayer, and Sun Microsystems. Switch and telecom equipment vendor partners include Lucent, Cisco, Nortel, Telcordia, Sonus, and Alcatel just to name a few. Flexible deployment, scalability, dynamic capabilities, and manageable configurations make the Xcipio lawful intercept product an outstanding and innovative approach to electronic surveillance and CALEA compliancy.

Award Description

The Frost & Sullivan Award for Technology Innovation is given to the company that has demonstrated technological superiority within its industry. This award recognizes the ability of the company to successfully develop and introduce new technology, formulate a well-designed product family, and make significant product performance contributions to the industry.

Research Methodology

To choose the recipient of this award, the analyst team tracks emerging and existing technologies, as well as R&D developments. This is accomplished through interviews with major market participants and extensive secondary research. Also considered are elements such as product launches, customer acceptance, market demand, and time to market. Finally, competitors are compared and ranked for relative position. Frost & Sullivan then presents the award to the company that received the number one industry rank.

Measurement Criteria

In addition to the methodology described above, specific criteria are used to determine the final competitor rankings in this industry. The award recipient has excelled based on one or more of the following criteria:

- Innovative technology design
- R&D development and resources
- New product/process introduction
- Early entry in a high-demand market
- Current and potential adoption rate
- Product or technology meets multiple needs and communications technologies

State of the CALEA Market

Market Engineering Measurements—Snapshot of the CALEA Market

Chart 1.1 displays the Market Engineering Measurements of the CALEA Telecommunications Market.

Chart 1.1

CALEA Telecommunications Market: Market Engineering Measurements (U.S.), 2002

Market Engineering Drives Market Strategy and Planning

Measurement Name	Measurement	Trend
Average Cost of a Wiretap	54,000	Rising 5 to 7 percent per year
Carrier Costs for CALEA implementation	$50,000 to $500,000 per switch	Stable
Available CALEA Solutions	Switch Hardware (Mediation)	
	Switch Software	
	Adjunct Box (Internal or external)	
Service Bureau Solution	CALEA solutions are increasing in terms of availability and technology compliance	
Carrier CALEA Responsibilities	Access and Delivery Functions of Call Identifying Information to LEA	N/A
Most common wiretap medium	Wireless phone or PDA	77 percent and growing
Top States for Wiretaps	New York, California & New Jersey	N/A
Number of Authorized Intercepts	Over 1300	Expected to climb
Major Offense for Intercept Targets	Drug or drug-related	N/A
Percentage of 2002 Federal Authorizations	38 percent	Growing
Percentage of 2002 State Authorizations	62 percent	Stable

Source: Frost & Sullivan, Administrative Office of the US Courts

History of CALEA

Background of the Act

In 1968, the United States Congress passed the Omnibus Crime Control and Safe Streets Act in an effort to protect the privacy of communications and establish uniform requirements for intercepting communications. In 1986, the United States Congress passed the Electronic Communications Privacy Act to establish a standard for intercepting electronic mail, cellular telephone calls, and paging devices.

In 1990, The United States Senate formed a Committee to study developments in communication technology and the right to privacy. A report was issued in 1991 that recommended that privacy protections be extended to wireless data, wireless LANs, and cordless telephones.

The United States Congress passed the CALEA Act in 1994 to require telecommunications carriers to cooperate in the interception of communications. On October 12, 2001, the US Congress passed the USA Patriot Act and further modified and expanded the requirements for CALEA. On June 30, 2002, CALEA finally went into effect. The lengthy delays in implementing CALEA did not reduce the number of last minute waivers filed by telecom carriers with the FCC.

Wiretapping History

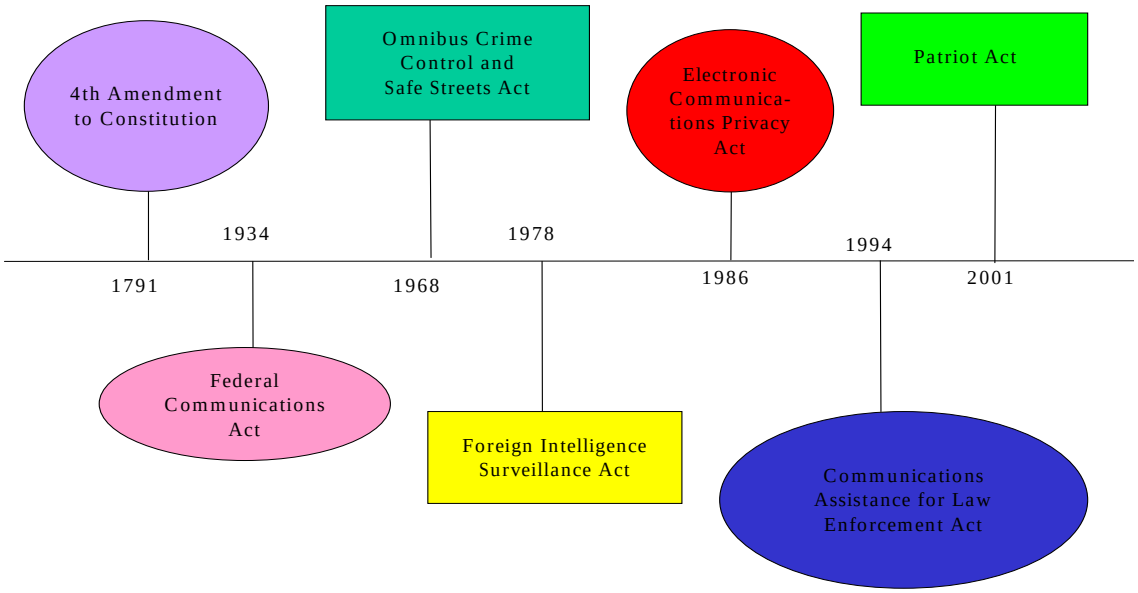
Wiretapping traces back well before CALEA legislation. In fact, shortly after the telegraph was invented in 1844 the U.S. Government monitored telegrams prior to and during the Civil War. Wiretapping also has a long history of debate within the U.S., with a common theme of balancing individual or civil rights, i.e. privacy, with the federal government and its emphasis on public safety.

Chart 1.2 displays the major pieces of federal legislation, which have had some impact on U.S. governmental wiretapping of the populace.

Figure 1-1 highlights the impact that rapid technological changes have made on the legal issues concerning wiretapping, notice how the seven major pieces of legislation go back over 200 years, yet three of these have occurred in the last 15 years. It also emphasizes the legal proponent and reasoning for each wiretap law.

Chart 1.2

U.S. CALEA Market: History of Legal Acts, 2003



Note: All figures are rounded. Source: Frost & Sullivan

Figure 1-1

Legislation, Proponent and Reasoning for Wiretapping Legislation, 1791-2001

Year	Legislation	Proponent	Reason
1791	4th Amendment to the Constitution	Citizens	Protect the Public from and restrict the power of the U.S. Government
1934	Federal Communications Act	Government	Regulate Communications Industry
1968	Omnibus Crime Control and Safe Streets Act	Government	Disrupt Organised Crime
1978	Foreign Intelligence Surveillance Act	Government	To be able to wiretap without a Title III warrant any individual characterized as a spy
1986	Electronic Communications Privacy Act	Citizens	Protect the public from unauthorized governmental searches through new electronic mediums
1994	Communications Assistance for Law Enforcement Act Government	To make wiretapping a much easier process for the Government	
2001	Patriot Act	Government	To make it easier to wiretap potential 'terrorists'

Note: All figures are rounded. Source: Frost & Sullivan

Figure 1-2 indicates the obligations each new law placed on the communications industry and the government.

Figure 1-2

Government and Service Provider Obligations for Wiretapping Legislation, 1791-2001

Year	Legislation	Government	Service Provider
1791	4th Amendment to the Constitution	Not allowed to conduct unreasonable searches and seizers, must have a search warrant	Not Applicable
1934	Federal Communications Act	Regulating interstate and foreign commerce in communication by wire and radio and make available to all U.S. citizens. Wiretaps do not need any court approval however evidence can not be used in court	The act Regulates: charges, classifications, practices, services, facilities, or other regulations for or in connection with intrastate communication service by wire or radio of any carrier
1968	Omnibus Crime Control and Safe Streets Act	Not allowed to conduct Wiretaps without a Title III Warrant, Wiretaps can now be used as evidence in a courtroom trial	Comply with all wiretaps that have an issued search warrant
1978	Foreign Intelligence Surveillance Act	Conduct wiretaps without warrant on potential spies	Assist Government with surveillance of potential Espionage Activities by U.S. or foreign citizens
1986	Electronic Communications Privacy Act	Government needs a search warrant for information gathered from monitoring radio paging devices, electronic mail, cellular telephones, private communication carriers, and computer transmissions	Assist Government with surveillance of new technology computer devices like the Internet only with written court order
1994	Communications Assistance for Law Enforcement Act	Later amendments to this act force the government to give $500 million to communications carriers in payment for their compliance with the order	Communications Carriers must make their networks CALEA compliant in order to enable wiretaps faster and more cost effectively for the U.S. Government
2001	Patriot Act	Increased interaction between CIA and FBI; government agencies must work together to stop terrorism	Communications Carriers must be prepared for increased governmental surveillance, cooperation is necessary

Note: All figures are rounded. Source: Frost & Sullivan

Below is commentary on each piece of legislation with concern to wiretapping, in chronological order:

- **4th Amendment to the Constitution:** On the heels of the revolutionary war this piece of legislation was put into place to protect the public against unreasonable search and seizure, common occurrences under British Colonial Rule. Interpretation of this Amendment is key to any debate or decision on wiretapping. Taken literally, the 4th Amendment doesn't forbid wiretapping lacking a search warrant, as the key points of the legislation are about physical searches of a person or their residence.

- **Federal Communications Act:** Prohibits interception and divulgence of wire communications. The FBI and other governmental investigative bodies have focused on the term and using the conjunction to justify massive amounts of wiretaps during J. Hoover's reign as director of the FBI. The FBI believed it was lawful to conduct wiretaps as long as the information collected was not made public or used in a criminal trial. Wiretaps where a major way for the FBI to collect information about other forms of admissible evidence during this time period.

- **Omnibus Crime Control and Safe Streets Act:** In Title III, also known as the federal wiretap act, intercepting wire or oral communications without any party's consent is allowed only through direct authorization of a court of competent jurisdiction. Also, only certain crimes could be investigated using wiretaps, and this legislation was aimed squarely at organized crime, as the list included murder, kidnapping, extortion, gambling, counterfeiting, and sale of marijuana.

- **Foreign Intelligence Surveillance Act:** Electronic surveillance of foreign agents allowed under secret court order, given probable cause that target is agent of foreign power, search warrant not necessary. Electronic surveillance conducted must conform to certain stipulations, the requirements for obtaining a court order and for reporting to the Attorney's Office are much less restrictive than those outlined by Title III. The Foreign Intelligence Surveillance Court grants court orders for a FISA wiretap.

- **Electronic Communications Privacy Act:** Extends Title III wiretap protections to wireless phones, email, and computer-computer communications. Extends requirement for subpoena, but not warrant, to pen registers.

- **Communications Assistance for Law Enforcement Act:** The primary purpose of the CALEA act is to clarify a telecommunications carrier's duty to assist law enforcement agencies with the lawful interception of communications and the collection of call-identifying information in a rapidly changing telecommunications environment. Following the act and industry protests, Congress stipulates funding for the carriers, which fell well short of what was needed for them to make the required changes. CALEA marked the first major retreat from providing privacy protections for telecommunications technologies in legislation.

- **Patriot Act:** This legislation, written hastily after September 11th, increases governmental powers under FISA (the Foreign Intelligence Surveillance Act). This allows increased surveillance of U.S. citizens, other lawful residents, and illegal aliens, under the pretext of potential international espionage. The Patriot Act also increases interaction between the CIA, FBI, and other governmental investigative units. This has the potential to cause skirting of wiretap laws previously put in place to protect privacy, as the FBI could avoid Title III by characterizing the suspect as a potential spy and having the CIA conduct the wiretap. This would make it possible to avoid a traditional court process for a warrant and get permission for surveillance through the FISA court.

Both the economic cost and the prevalence of governmental wiretaps has greatly fluctuated over the past fifty years. Prior to the Omnibus Crime Control and Safe Streets Act of 1968, the government abused the privacy rights of citizens, performing illegal wiretaps at its discretion. In the previous thirty years, the administrations of Roosevelt, Truman, Eisenhower, Kennedy and Johnson conducted over 10,000 such illegal wiretaps. By contrast, after passage of Title III, less than 8,000 legal wiretaps were conducted in the next thirty years. This is an especially stark contrast because of the fact that the telephone system in the United States grew considerably between the 1930s and the 1990s.

The "Punch List" and Legal Requirements

CALEA specifically requires telecommunications carriers to intercept the following:

- Digital communications of all types.
- Call Identifying Information - origin, direction, destination, and termination of each communication generated or received by means of any equipment, facility, or service.
- Electronic messaging software that enables sharing of data, images, sound, writing, among computer devices.
- Information Services - generating, acquiring, storing, transforming, processing, retrieving or using telecommunications.
- Telecommunications support - products, software, or service used by a carrier for internal signaling or switching.

Carrier requirements under CALEA include:

- Isolate, enable, identify, intercept, and deliver all wire and electronic communications as required by lawful authorization
- Carriers are responsible for consulting with manufacturers of their transmission and switching equipment to ensure that current and planned equipment comply with CALEA requirements.

The FCC requires that wireline, cellular, and broadband PCS carriers implement all electronic surveillance standards, including two contested standards, packet communications and location information. "Information services" is not included in the definitions of CALEA. There are many cloudy issues around IP traffic because of the definitions set in CALEA, and the definition of "information services." Six additional requirements, known as "punch list" capabilities, requested by the Department of Justice and the Federal Bureau of Investigation include:

The "PUNCH LIST"

Dialed digit extraction-digits dialed by a subject after initial call setup is complete

Party Hold/Join/Drop-identifies parties on conference calls

Subject Initiated Dialing and Signaling-Dialing and Signaling by means of flash-hook and feature keys

In-Band and Out-of-Band Signaling-Tones, network signals, and messages

Subject Initiated Conference Calls-Content of conference calls

Timing Information-Call-identification correlated with content

All telecommunication carriers that operate within the U.S. are required to participate in the CALEA program. Other communication carriers such as Internet Service Providers, or ISPs, along with paging or electronic messaging companies are also required to participate in criminal investigations. Network equipment vendors are also responsible for creating CALEA capable products. When called upon by governmental agency communications carriers must:

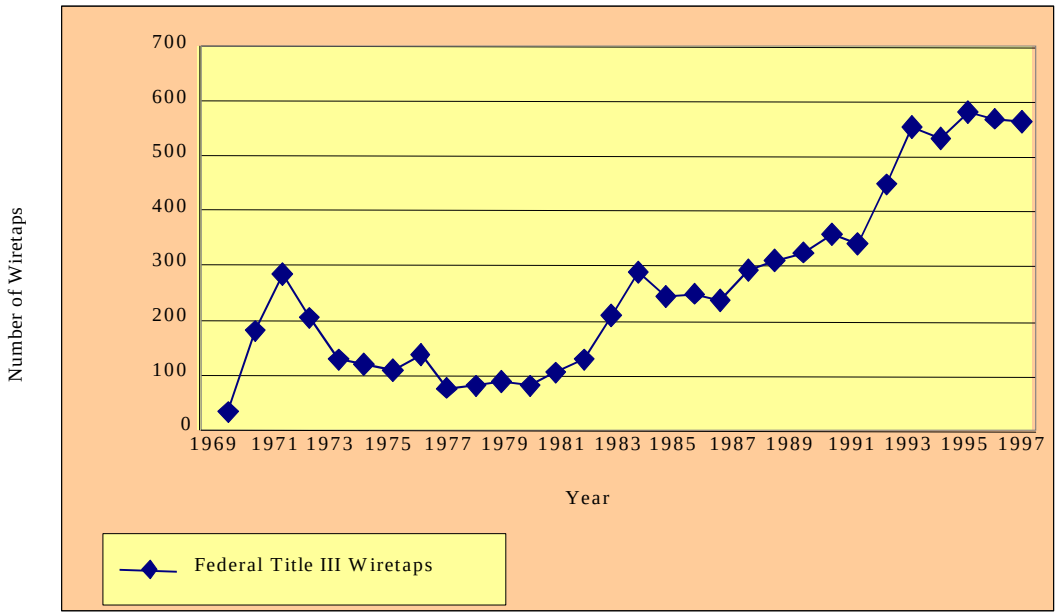
‘Pursuant to a court order or other lawful authorization, carriers must be able to: (1) expeditiously isolate all wire and electronic communications of a target transmitted by the carrier within its service area; (2) expeditiously isolate call-identifying information of a target; (3) provide intercepted communications and call-identifying information to law enforcement; and (4) carry out intercepts unobtrusively, so targets are not made aware of the electronic surveillance, and in a manner that does not compromise the privacy and security of other communications.

If a communications carrier doesn't fully comply with a court order for surveillance, a fine of up to $10,000 a day per intercept may be imposed. To date, no carrier has ever been fined; the $10,000 stipulation has been used by the FBI as leverage to get carriers to work with them on difficult cases.

Federal wiretapping and surveillance has seen an increase over the past decade. With recent terrorism, war, and homeland security issues, there is even more focus on protecting the homeland through surveillance and criminal investigations. Chart 1.3 shows the history of Federal "Title III" wiretapping in the U.S.

Chart 1.3

Federal Title III Wiretaps, 1968-1998



Note: All figures are rounded. Source: Frost & Sullivan

Types of Surveillance

Law enforcement agencies can perform a number of types of surveillance, but all must be approved through a court order. The following defines the different types of electronic surveillance:

- Pen Register
- Trap and Trace
- Interception (Title III)

Pen register involves the recording of call identifying information for all call originated by the subject or suspected criminal. In short this is recording phone numbers of people that the target is calling. Trap and trace involved the call identifying information for all calls received by a subject or suspected criminal. This involves recording phone calls of people calling the target. Lastly, interception allows law enforcement to listen to the conversations of the subject, as well as receive full access to the call identifying information. Approximately 90 percent of all surveillance orders are of the first two types (pen register & trap and trace). Federal law and the laws of forty-two states only allow the use of the third technique in the investigation of serious criminal offenses, and when other techniques have not worked, will not work, or are too dangerous. Interception surveillance evolves around "Title III" of the

Omnibus Crime Control and Safe Streets Act of 1968 and the Federal Intelligence Surveillance Act of 1978.

CALEA Funding and Resources

CALEA Funding and Associated Costs

In short, the funding for the implementation of the CALEA program in the past came directly from the U.S. Government ($500 million from the FBI CIS). Besides direct appropriations from Congress, the CALEA program has also received funding from the Justice Department, U.S. Customs Service, and the U.S. Postal Service. Figure 1-3 details previous allocations for the CALEA project.

Figure 1-3

CALEA Compliance Funding: Fiscal Years 1997-2001

Funding Source	Year	$ Dollars
Direct Appropriation	1997	60,000,000
Department of Justice Working Capital Fund	1997	40,000,000
United States Customs Service Transfer	1997	1,580,270
United States Postal Inspection Service Transfer	1997	1,000,000
Direct Appropriation	2000	15,000,000
Supplemental Appropriation	2000	181,000,000
Direct Appropriation	2001	200,976,876
Total Deposits as of end of 2001	2001	499,557,146

Source: CALEA Report to Congress, December 17th 2001 Prepared by the FBI

Usage of the CALEA program is funded by the State or Federal agency that requests a wiretap. Figure 1-4 details several statistics on the use of wiretaps within the U.S.

Figure 1-4

Wiretap Statistics for 2001 and 2002

Attribute	Numeric Metric
Federal Wiretaps Authorized in 2002	497
State & Local Wiretaps Authorized in 2002	861
Total 2002 Authorized Wiretaps	1358
Average Persons whose communications were intercepted per wiretap 2001	86
Average Length of a wiretap in 2002 in days	29
Average Length of a wiretap in 2001 in days	27
Number of Wireline Wiretaps for 2002	153
Number of Wireless Wiretaps for 2002	971
Number of Business Wiretaps for 2002	37
Combination Wiretaps for 2002	85
Other Wiretaps, includes prisons, pay phones and public areas	83

Source: 2002 Wiretap Report Administrative Office of the United States Courts

Figure 1-5 details the individual states' use of wiretaps. Notice that only 41 out of the 50 U.S. states currently allow wiretaps, however federal investigations may use wiretaps within the remaining states.

Figure 1-5

Wiretap Application Statistics by State for 2002

State	Wire Taps
New York	404
California	143
New Jersey	81
Pennsylvania	79
Maryland	54
Florida	37
Illinois	25
The other 34 states that allow wiretaps, along with District of Columbia, and the Virgin Islands	182
Total State Wiretaps	1005

Source: 2002 Wiretap Report Administrative Office of the United States Courts

CALEA costs are becoming more of a pressing issue since September 11th. After 9/11, CALEA compliant moved to the top of the priority list, in an effort to provide LEAs the access and functionality to secure the homeland and pursue terrorist investigations. Carriers are faced with costs ranging from $50,000 to $500,000 per switch to meet the six "punch list" items, and general maintenance and upkeep may range anywhere from $100,000 to $400,000 annually. These costs in the eyes of many carriers cannot be justified in the current economy, as well as are hard to swallow knowing there may be very little intercept requests from law enforcement.

The wireless industry is also facing severe costs to implement CALEA compliant switching and provisioning. Several wireless vendors and other authorities have stated the total wireless industry's implementation costs to be an estimated $50.0 to $60.0 million. On the other hand, the wireline industry are faced with higher costs totaling an estimated $300.0 to $400.0 million in implementation costs. Implementation costs include the hardware (Mediation servers, routers, wiring, dedicated lines), one-time capital costs, and other initial fees. Operating costs are another ball game. Some estimates in the industry indicate operating costs of $100,000 to $400,000 annually per carrier, as noted earlier. While estimations of operating costs have been stated here and there, there are a number of factors that will decide operating expenditure costs. Those include the following:

- Number of switches, switching center locations, and nodes in the network
- Vendor or number of switching and equipment vendors to work with
- Number of upgrades needed or administered each year
- The amount of change and legal requirements based on CALEA law
- The complexity of the current network (VoIP, wireless data, multiple platforms)
- Resources available for administering call events, and managing the lawful intercept provisioning process
- The choice of CALEA solution and vendor (switch-based, adjunct-based, service bureau)

Because the reimbursements that Congress passed previously are pretty much depleted, new and emerging carriers will have to incur the full costs of implementing a CALEA solution. Figure 1-6 details governmental spending on CALEA with carriers and switch vendors through the end of 2001, aka the telecommunications carrier compliance funding from 1997-2001.

Figure 1-6

Telecommunications Carrier Compliance Funding: FY 1997-2001

Payments to Carriers Purchasing CALEA compliant solutions	Year	$ Dollars
Nortel via Ameritech for NAO10 CALEA functionality	1999	15,000,000
Nortel via Ameritech for NAO11 CALEA functionality	2000	5,000,000
Nortel via Ameritech for NAO12 CALEA functionality	2000	5,000,000
Nortel via Air Touch Cellular (Now Verizon) for MTX-08 & MTX-10 CALEA functionality	2000	26,000,000
Nortel via Nextel for GSM 10 CALEA functionality	2001	13,400,000
Nortel via Ameritech for 501 CALEA functionality	2001	18,000,000
Motorola via Nextel for 9.15 CALEA functionality	2001	25,000,000
Siemens via Loretto for 22 CALEA functionality	2001	15,000,000
AG Communications System (AGCS) via Verizon for SVR 4004 CALEA Functionality	2001	25,000,000
Lucent via Verizon for SVR 4004	2001	95,000,000
SBC for partnership role in CALEA testing	2001	19,721
Motorola via Verizon for 15 CALEA functionality	2001	20,000,000
Ameritech for partnership role in CALEA testing	2001	126,850
Governmental Late Payment penalties to various carriers and vendors	2001	5,198
Nortel via Verizon for DMS-MTX CALEA functionality	1999	7,000,000
Nortel via Ameritech for DMS-10 CALEA functionality	2000	2,900,000
Nortel via Ameritech for DMS-100 functionality	2000	5,000,000
Nortel via Nextel for DMS-MSC CALEA functionality	2000	4,500,000
Verizon for partnership role in CALEA testing	2000	97,801
Lucent via Verizon for CALEA functionality on the 5ESS	2000	15,000,000
AGCS via Verizon for 5ESS CALEA functionality	2000	5,000,000
Siemens via Loretto for CALEA functionality on EWSD	2000	20,000,000
Siemens via Lorretto for CALEA functionality on DCO	2000	5,000,000
Motorola via Verizon for EMX2500/5000 CALEA functionality	2001	10,000,000
Lucent via Verizon for Autoplex-1000 CALEA functionality	2001	60,000,000
Verizon for partnership role in CALEA testing	2001	310,000
Total Spent by end of year 2001	2001	397,359,570
Budgeted Allocation to Carriers for 2002	2002	102,197,576

Source: CALEA Report to Congress, December 17th 2001 Prepared by the FBI

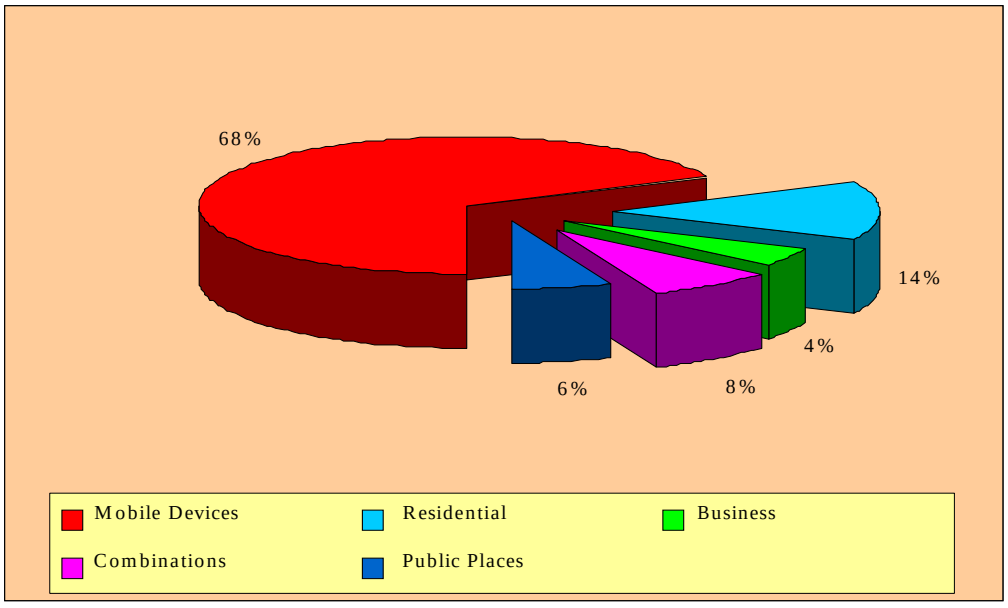
Several RBOCs report that conducting wiretaps for the FBI and other authorized state and federal agencies is very expensive and that the best they hope for is to break even on costs versus reimbursements by the government. Most are expected to incur costs over the long-run. Maintenance and monitoring of wiretaps is very costly, as network engineers must make sure that all pertinent information is reaching the investigative body in a timely and efficient manner. A dedicated line must also be provisioned rapidly from the central office to the government agency, so that information collected reaches the investigators and no one else has access to it. Finally, during investigations time is crucial and many man-hours, including overtime, are invested by the carriers to get wiretaps up and running rapidly. The carriers consider this good corporate citizenship and do it knowing it often ends up being an unprofitable venture for them.

Wiretapping Facts and Figures

Chart 1.4 displays the U.S. Wiretaps by Location.

Chart 1.4

Wiretaps by Location, 2001

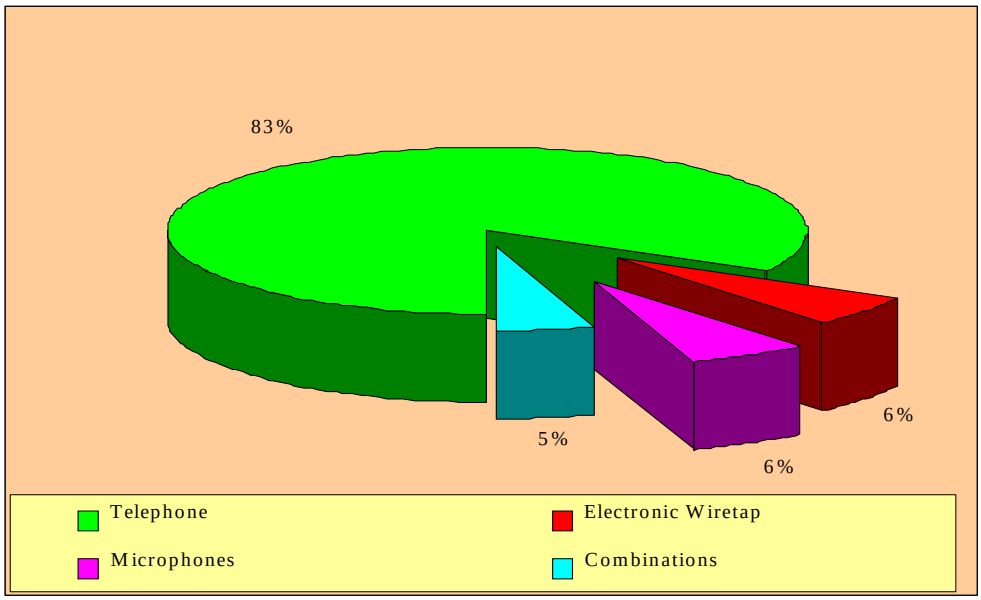


Source: 2001 Wiretap Report Administrative Office of the United States Courts

Chart 1.5 displays the U.S. Wiretaps by Medium.

Chart 1.5

CALEA Wiretaps by Medium, 2001

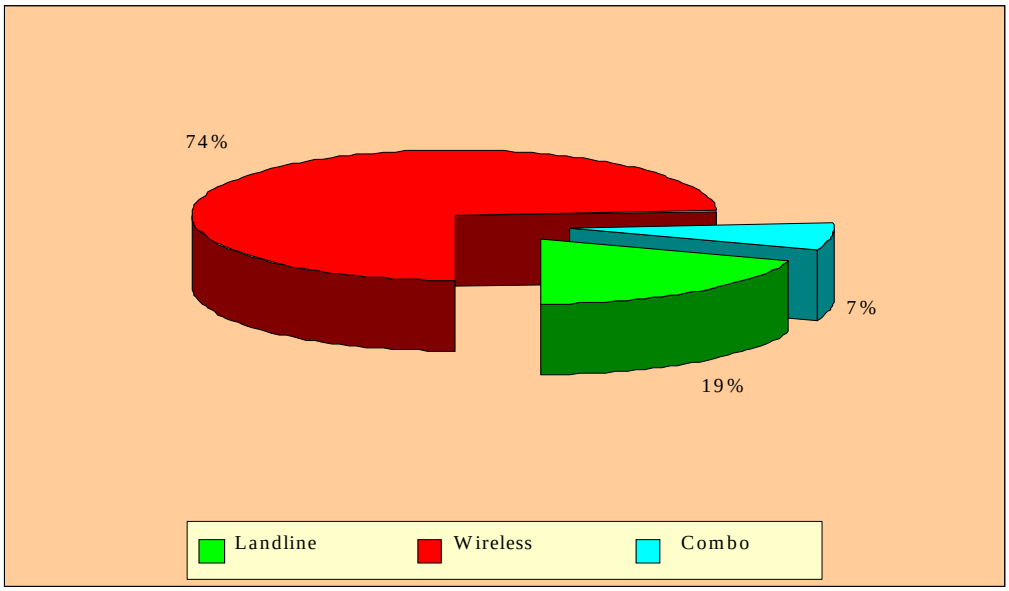


Source: 2001 Wiretap Report Administrative Office of the United States Courts

Chart 1.6 displays the U.S. Wiretaps by Type of Device. Chart 1.7 displays the U.S. Wiretaps by Electronic Devices broken down by segment.

Chart 1.6

Wiretaps for Electronic Devices by Segment for 2001

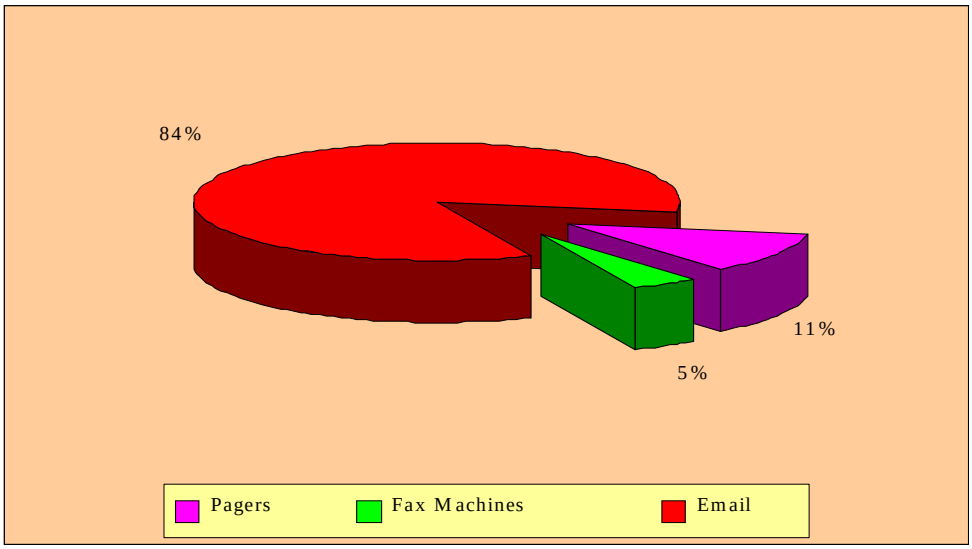


Source: 2001 Wiretap Report Administrative Office of the United States Courts

Chart 1.8 displays the U.S. Wiretaps by Type of Criminal Investigation.

Chart 1.7

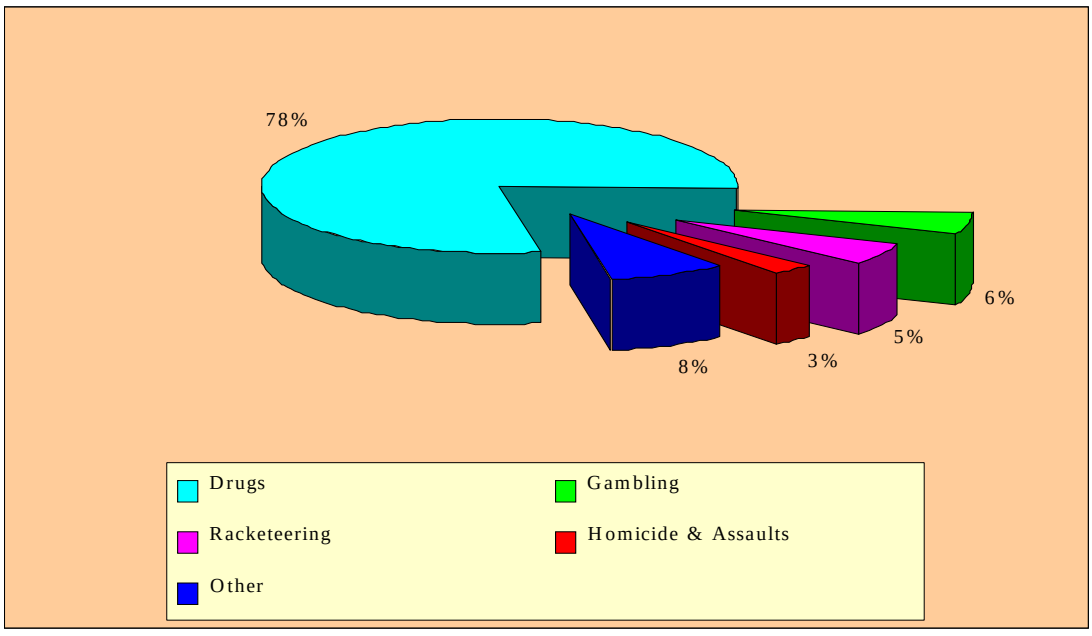
Wiretaps for Electronic Devices by Segment for 2001



Source: 2001 Wiretap Report Administrative Office of the United States Courts

Chart 1.8

2001 Wiretaps by Type of Criminal Investigaticon



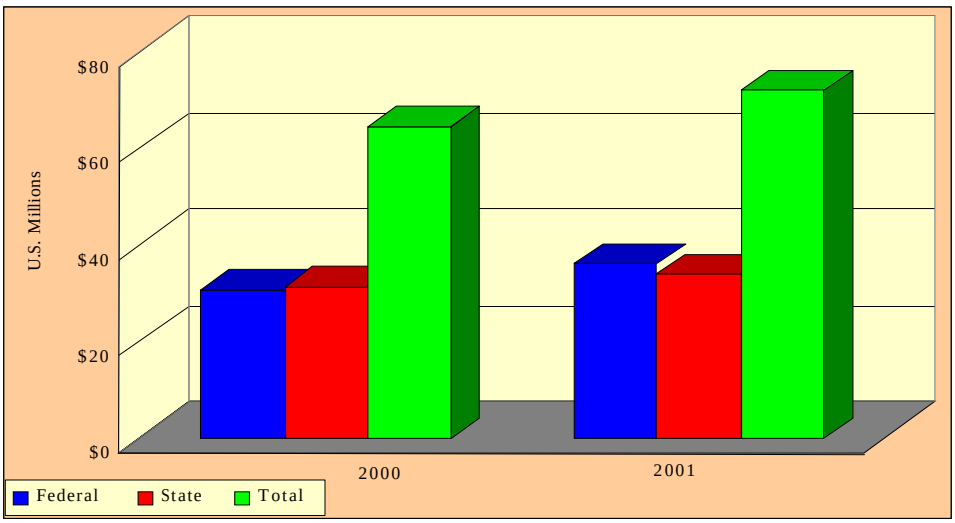
Source 2001 Wiretap Report Administrative Office of the United States Courts

Wiretapping Expenditures in the U.S.

Chart 1.9 displays the U.S. Wiretap Government Spending by Segment. Chart 1.10 demonstrates the U.S. Forecast of Total U.S. Wiretap Spending.

Chart 1.9

Governmental Spending on Wiretaps for 2000 and 2001 by Segment



Source: 2001 Wiretap Report Administrative Office of the United States Courts

Chart 1.10 demonstrates the U.S. Forecast of Total U.S. Wiretap Spending.

Chart 1.10

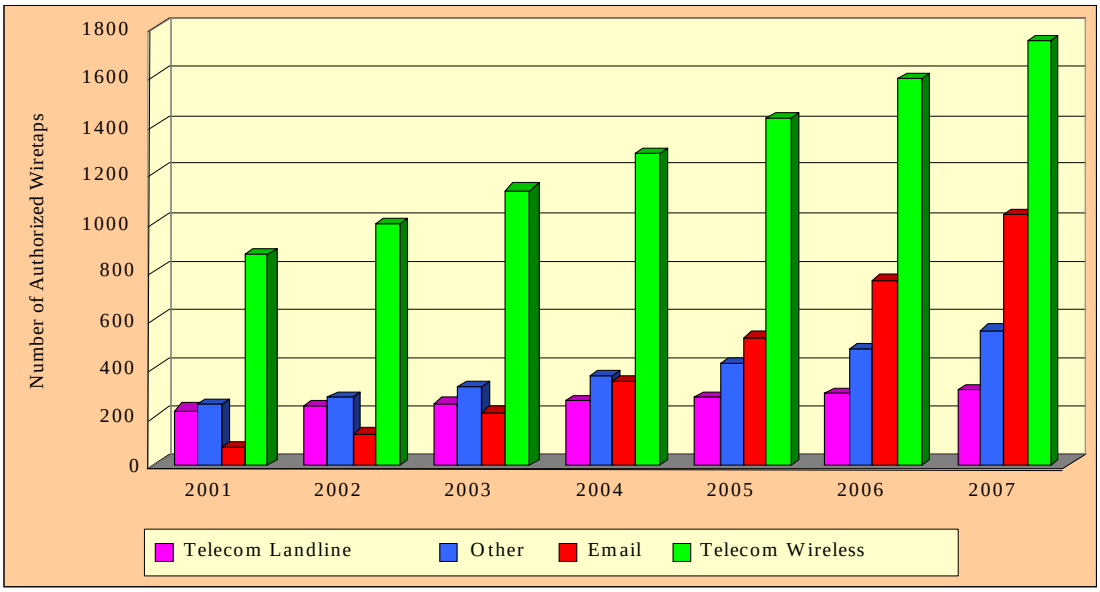
Forecast of Total U.S. Wiretap Spending, 2002-2007

Source: 2001 Wiretap Report Administrative Office of the United States Courts and Frost & Sullivan

Chart 1.11 details the U.S. Forecast of CALEA Wiretaps for both the U.S. Federal and State Agencies.

Chart 1.11

Forecast of CALEA Wiretaps for both U.S. Federal and State Agencies, 2001-2007



Source: 2001 Wiretap Report Administrative Office of the United States Courts

CALEA Technical Analysis

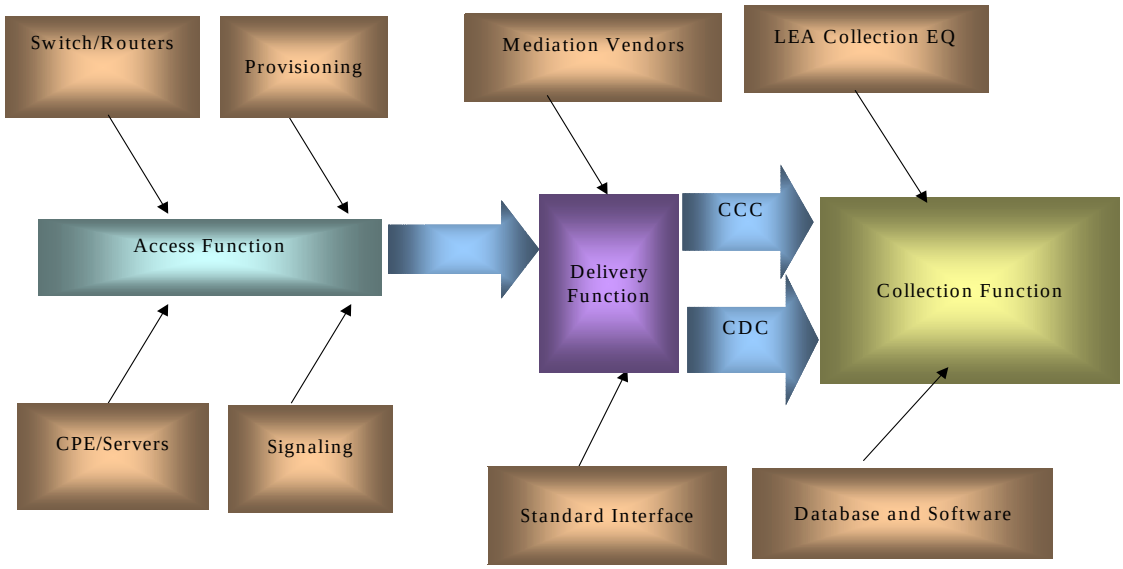
Basic CALEA Analysis (TDM & PSTN)

CALEA requires telecommunications carriers (Wireline and Wireless) to provide the LEA with access to intercept. This includes all wire and electronic communications to and from the target, call identifying information and the correlation between. This also must be performed with minimum interference of services and with the protection of customer privacy. This involves a number of areas of functionality within a carriers switch and provisioning system. In the past carriers only had to segregate the twisted pair of the targeted individual, now this is not the case. Chart 1.12 displays a PSTN CALEA diagram. As shown in Chart 1.12, there are three basic areas of functionality in a typical CALEA system architecture. Those include the following:

- The Access function (Carrier)
- The Delivery function (Carrier)
- The Collection function (LEA)

Chart 1.12

PSTN CALEA Architecture Diagram



Note: All figures are rounded. Source: Frost & Sullivan

Carriers are responsible for both the access and delivery function, while the LEA is responsible for the collection function. The administering and provisioning of the intercept call/data event is one of the first steps after the court order is received. The access function is performed at the switch, which records the call record information. Changes exist depending on the switching vendor and, also the type of transmission protocol (Leased lines, TCP/IP over x.25 or ISDN, etc). The access function consists of one or more intercept access points and defines the interface to the switch (Class 5 or softswitch).

The delivery function is responsible for carrying the lawful intercept to the collection point. The delivery function is based on whether the call is delivered over IP or PSTN, and usually includes servers, mediation devices, routers, and other equipment that collects the call information and data according to the U.S. J-STD-025/J-STD-025A standard if carried over an IP network. Each switch vendor has developed its own transport protocols for delivering the messages to the LEA (Law Enforcement Agency). The delivery must be performed over two separate channels, one for the call data (Call Data Channel or CDC) and the other for call content (Call Content Channel or CCC). Also important is the system's ability to deliver to five separate LEAs for a single intercept at any given time. These five LEAs cannot know about each other when the intercept delivery is taking place. The carrier must provide dedicated and secure transmission to the LEA locations(s).

The collection function houses the LEAs' (Law Enforcement Agency) computer system, software, and database system. The collection function allows for the collection of call content and data, as well as the analysis and interpretation of the call content and data. There are numerous solutions and vendors that offer collection equipment and software to the LEAs. Frost & Sullivan must emphasize that the collection function is the responsibility of the LEA.

The Court Order Process

Lawful Intercept requests may be court ordered on the following two collection areas:

- Call Data - includes call identifying information to or from intercept target
- Call Content - includes call content to or from intercept target

To incorporate CALEA requirements within a carriers network, carriers will require CALEA administration and control software, mediation device(s) or delivery host equipment, and CALEA application equipment and software. Large carriers will generally administer one to three individuals responsible for provisioning and overseeing the administration of CALEA compliancy. There is also the option to fully outsource the CALEA function through a service bureau or mediation vendor such as Fiducianet or VeriSign.

Wireless Analysis

CALEA remains to be an important issue for the wireless industry including both wireless and PCS vendors. The FCC extended the deadline for carriers to become compliant on June 30th, 2002. No one carrier met the full six "punch list" compliancy on June 30th. Differences in protocols, architecture, technology standards, and networks has made wireless CALEA compliancy even more difficult. In response to this, the FCC granted wireless/PCS carriers two-year waivers from the deadline for those showing that the technology available is not ready to comply with the law. The FCC got flooded with requests for the extension prior to the June 30th deadline. In fact, in August of 2002, over 300 carriers had requested extensions to prolong compliancy and to extend time to design a network solution. This clearly shows the industry is not ready for full compliancy on the "punch list" items, especially within the wireless industry.

Because wireless devices are the most commonly wiretapping medium, wireless vendors are facing great pressures to meet CALEA intercept rules. Wireless data intercepts are growing in number because of the growth in wireless messaging, wireless email, text paging, wireless web, and other forms of wireless data. Several vendors have already released certain phases to comply with wireless data intercepts including SS8 Networks and Verint Systems.

Wireless intercepts will depend on the call origination and termination, as well as how the call travels through the network to complete the call. For example, a long distance call from a wireless caller to another wireless caller will travel through the PSTN network. Also, a call from a wireless caller to a wireline caller may travel through various service provider networks before it reaches its final destination to the wireline caller. Intercepting wireless voice calls is very similar to intercepting traditional wireline calls, so that is not the pressing issue at this time.

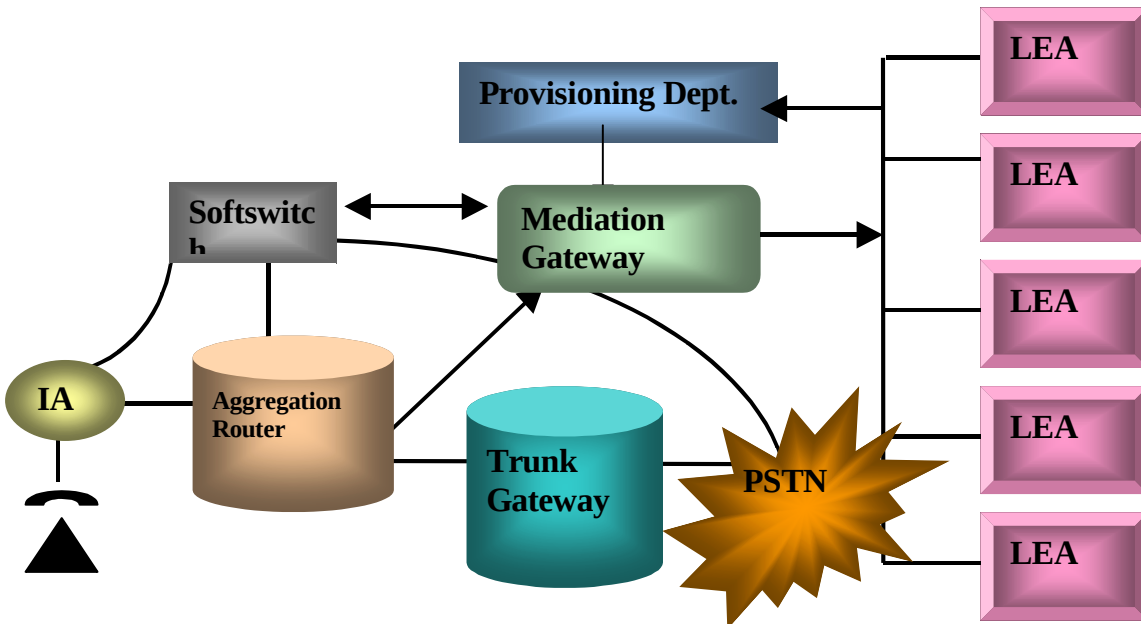
The pressing issue is dealing with wireless text messaging, wireless web, and wireless email intercepts. More will be discussed about this in the IP section of this study because these services are a form of wireless data, which travels through an IP or packer-based transmission.

Packet & IP-Based Analysis

In an IP Network, lawful intercept is in the early stages of architecture development. There are vendors that provide solutions for the access, delivery, and collection function of CALEA. Chart 1.13 demonstrates one example of an IP-based network and CALEA compliance.

Chart 1.13

IP Network CALEA Architecture Diagram



Source: Frost & Sullivan & CALEA Industry Organizations

The process for lawful intercept is as follows. A LEA will provide the court order to the appropriate carrier's provisioning department. The provisioning department will provision the requirements set by the court order, whether it includes call data or both call content and call data. The mediation gateway receives the changes set by the provisioning department, and this information is sent to the softswitch. The softswitch communicates directly with the interface access device (IAD), and the aggregation router. The IAD collects call content and data and sends it to the switch or aggregation router. The aggregation router separates the voice packets and sends the packets directly to the mediation gateway. The call content information is sent to the softswitch, which is then sent to the mediation gateway. The mediation gateway is responsible for preparing the call content and call data in a specific format, which will be sent to the LEA office. The LEA office receives the call content information separate from the call data information. Different carriers use varying formats to send the CCC and CDC to the LEA. It is important that carriers work closely with the LEAs to coordinate the delivery of call content and data to the LEA.

CALEA capabilities for VoIP are in the beginning stages of development. Prior to September 11th, neither the government nor the service providers were concerned about the lack of CALEA VoIP capabilities. Thus, VoIP providers are in a unique situation: They are not technically subject to CALEA, nor do they have to comply with the FCC's 1999 technical requirements, because they were never defined as telecom carriers. Until legislation is passed dealing specifically with wiretapping for VoIP providers (or until CALEA is amended to include VoIP) the government must request the tapping of VoIP networks on a case-by-case basis. It is expected that the FCC and FBI will be pushing this issue as VoIP becomes more prevalent. Carriers are becoming more prepared to provide lawful intercept in a packet network.

Taken literally, the CALEA legislation made no mention of VoIP, so many carriers were not concerned with compliance. On the other hand, opportunistic vendors such as SS8 Networks, VeriSign, and Jasomi Networks have begun to develop VoIP CALEA solutions. Using clever marketing ploys, they refer to a section of the CALEA act that stipulates a November 19, 2001 deadline for packet-switched networks. (This deadline has been repeatedly pushed back and is not in effect and was aimed at wireless networks not VoIP.) Most carriers who use VoIP are not very concerned about possible legal action and fines for not being CALEA capable, as most wiretaps are conducted on the local loop of telecom networks, a portion of the telecom market that facilitates VoIP the least.

However, there are major obstacles to be overcome. After September 11th a more theoretical view of the CALEA act has been taken by the U.S government, along with the passage of the Patriot Act, putting an emphasis on CALEA legislation applying to all new forms of technology and communication.

The following are the key challenges to industry wide VoIP CALEA solutions:

- Lack of a market for CALEA VoIP solutions: Without governmental demand for VoIP wiretaps, vendors have no impetus to create solutions. Carriers have no incentive for early adoption as it would not improve business performance in the least and the possibility of fines for non-compliance is minuscule.
- Lack of standard protocol for VoIP: The two major standards for VoIP are H.323 and SIP (Both establish telecommunications sessions over packet media, hence H.323 GateKeeper and SIP Proxy); many others are also used. Without a standard product, development is more difficult and less likely to be profitable.
- Difficulties in determining whether the packet communications is an "information service" or a "telecommunications service", by observation or on a packet-by-packet basis.
- VoIP call routing: Due to the nature in which VoIP calls are routed, intercepting all packets sent and received by an individual is difficult unless the wiretap was conducted at a point in the network that all traffic to or from an individual must pass through. Often times, this is at the local loop, where a traditional PSTN call is then converted to VoIP. With numerous solutions and capabilities in place for CALEA PSTN wiretaps, why would the government or carriers struggle with VoIP issues when they can avoid them by wiretapping calls directly from the local loop, before the call is converted to VoIP?
- Potential encryption of VoIP calls: Current privacy software is available to encrypt VoIP calls inexpensively. Encryption will probably be an ongoing challenge for VoIP wiretaps, as new encryption products will follow advances in wiretap capabilities and vice-versa. Currently using the Internet encryption format of public and private keys, encrypted VoIP calls cannot be understood by a wiretap without one of the individuals on the call divulging the encryption key to the investigative body.
- Lack of VoIP use within the local loop: Currently VoIP is most popular with U.S. carriers for international long distance, where it accounts for a mere 5 percent of total international traffic. It is less popular for domestic long distance, and even less for local traffic. Most wiretaps are conducted at the local loop level, with very few exceptions, so VoIP CALEA solutions are not extremely necessary at the current time.

Future of IP and CALEA

There are several obstacles to overcome for CALEA VoIP solutions. The majority of wiretaps are conducted on the local loop, a place in telecommunications networks where VoIP is used the least. A lack of a potential market for VoIP CALEA wiretaps has caused vendors and potential vendors to not develop solutions or to create only rudimentary capabilities.

Resourceful criminals using PC-to-PC VoIP with encryption can also make it virtually impossible for wiretapping to effectively elicit any call content information.

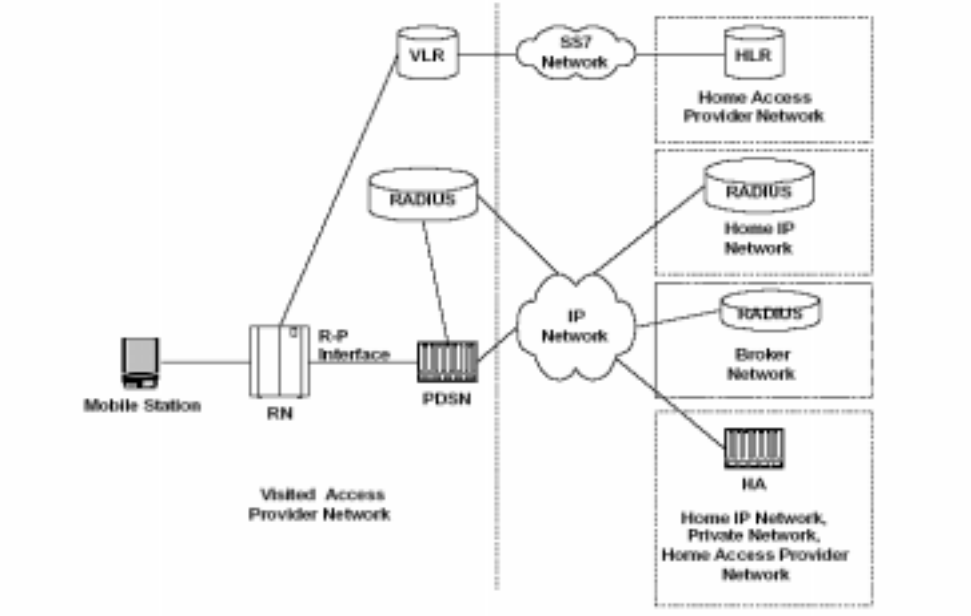
In the future, VoIP will become more CALEA compliant. This will happen due to several potential reasons. First, legislation and government funding can easily force this issue. Second, any publicity about the lack of governmental capabilities in this area could create a large public controversy that would put pressure on carriers and the government alike to take action. Finally, communications networks are slowly and steadily moving towards VoIP and eventually CALEA wiretapping capabilities will be necessary.

Architecture of Wireless IP

Chart 1.14 displays a typical wireless IP architecture for CALEA, based on feedback from the Telecommunications Industry Association and members from the Joint Experts Meeting for CALEA.

Chart 1.14

Mobile IP CALEA Network



Source: Telecommunications Industry Association, Joint Experts Meeting Feedback

Acronyms and Definitions

CALEA - Communications Assistance for Law Enforcement Act

CCC - Call Content Channel

CDC - Call Data Channel

CDRs - Call Detail Records

DEA - Drug Enforcement Agency

DOJ - Department of Justice

FBI - Federal Bureau of Investigation

FCC - Federal Communications Commission

FISA - Foreign Intelligence Security Act

IAD - Integrated Access Device

IAP - Intercept Access Point

IP - Internet Protocol

ISDN - Integrated Services Digital Network

ISP - Internet Service Provider

LAES - Lawfully Authorized Electronic Surveillance

LANs - Local Area Networks

LEA - Law Enforcement Agency

LI - Lawful Intercept

MSAG - Master Street and Address Guide

PSTN - Public Switched Telephone Network

PSAP - Public Safety Administration Point

SMS - Short Message Service

TIII - Title Three

CALEA Associations and Organizations

CALEA Compliancy Organizations

Federal Communications Commissions, CALEA Division - http://www.fcc.gov/calea/

FBI CALEA Implementation Section (FBI CIS) - http://www.askcalea.com

Organizations and Associations

Electronic Privacy Communications Center - http://www.epic.org/privacy/wiretap/calea/calea_law.html

International Softswitch Consortium (ISC) - http://www.softswitch.org

Telecommunications Industry Association (TIA) - http://www.tiaonline.org

North American Network Operators' Group (NANOG) - http://www.nanog.org

Global Lawful Intercept Industry Forum (GLIIF) - http://www.gliif.org

Cable Labs (PacketCable) - http://www.cablelabs.org

Personal Communications Industry Association (PCIA) - http://www.pcia.org

Alliance for Telecommunications Industry Solutions (ATIS) - http://www.atis.org

EuropeanTelecommunications Standards Institute (ETSI) - http://www.etsi.org

Universal Wireless Communications Consortium - http://www.uwcc.org

Cellular Telecommunications Industry Association (CTIA) - http://www.ctia.org

The Standards

J-STD-025ATIA (wireline and wireless)

J-STD-025BTIA (In the works)

PacketCable TMCableLabs

Packet and VoIPInternational Softswitch Consortium

PagingPCIA

Other Resources

TheFederal Register for CALEA rulings and orders.