RL30677

CRS Report for Congress

Digital Surveillance: The Communications Assistance for Law Enforcement Act and FBI Internet Monitoring

Updated January 25, 2001

Richard M. Nunno
Specialist in Information Technologies
Resources, Science, and Industry Division



Prepared for Members and Committees of Congress

Digital Surveillance: the Communications Assistance for Law Enforcement Act and FBI Internet Monitoring

Summary

The Communications Assistance for Law Enforcement Act (CALEA, P.L. 103-414, 47 USC 1001-1010), enacted October 25, 1994, is intended to preserve the ability of law enforcement officials to conduct electronic surveillance effectively and efficiently despite the deployment of new digital technologies and wireless services that have altered the character of electronic surveillance. CALEA requires telecommunications carriers to modify their equipment, facilities, and services, wherever reasonably achievable, to ensure that they are able to comply with authorized electronic surveillance actions.

The modifications, originally planned to be completed by 1998, have been delayed due to disagreements among the telecommunications industry, law enforcement agencies, (led by the Federal Bureau of Investigation (FBI)), and privacy rights groups, over equipment standards, and other technical issues. The amount of federal funds to be provided to the telecommunications carriers for implementation of CALEA, which carriers are eligible to receive those funds, and concerns over privacy rights of individuals, have also impeded implementation.

After receiving petitions from the industry and the FBI over the dispute, the Federal Communications Commission (FCC) in 1999 ruled in favor of most of the FBI's requests to require carriers to implement upgrades to their telecommunications networks (The FCC did extend the deadline for some of the upgrades requested by the FBI). This decision resulted in lawsuits being filed by industry and privacy rights groups. In August 2000, a federal appeals court upheld parts of the FCC's decision, but remanded most of it back to the FCC for reconsideration.

CALEA originally authorized $500 million to be distributed to telecommunications carriers for implementation. After enactment, industry and federal cost estimates increased, reaching $2 billion to $5 billion by 1999. Funding for CALEA was postponed for several years. To date, a total of $299 million has been appropriated to the Department of Justice to reimburse telecommunications carriers implementing CALEA, but has not yet been released.

The ongoing CALEA debate has found a renewed interest in Congress in connection with revelations about the FBI's efforts to monitor Internet communications using a computer system called Carnivore. Privacy rights issues related to Internet monitoring are similar to those in the CALEA debate because the format of data that can be collected from Internet communications is increasingly being used in telephone communications. Privacy rights groups believe that recent court rulings overturning portions of the FBI's CALEA requirements will set a precedent for future Internet monitoring rules.

Given that CALEA has still not been implemented six years after enactment, and law enforcement's digital surveillance actions are increasing, some question whether CALEA was ever necessary. Others argue that other technologies may still be used to circumvent the ability of law enforcement to perform wiretaps.

Contents

Background 1
Some Technical Terms 1

CALEA's Main Provisions 2

Major Events Following Enactment of CALEA 4
Initial Delays 4
The FBI's "Punch List" 5
Capacity Requirements 5
FCC Actions 6

Issues for Congress Regarding CALEA 7
Funding 8
Equipment and Standards 9
Impact on the Telecommunications Industry 10
Is CALEA Necessary? Is it Effective? 12
Privacy Issues Associated with CALEA 13

The Internet Dimension: The FBI's Carnivore System 14
Privacy Issues Associated With Internet Monitoring 15

Relevant Legislation in the 106th Congress 17

List of Figures

Figure 1. Total Federal and State Wiretap Authorizations 11

Digital Surveillance: The Communications Assistance for Law Enforcement Act and FBI Internet Monitoring

Background

In the early 1990s the Federal Bureau of Investigation (FBI) asked Congress for legislation to assist law enforcement agencies to continue conducting electronic surveillance. The FBI argued that the deployment of digital technologies in public telephone systems was making it increasingly difficult for law enforcement agencies to conduct electronic surveillance of communications over public telephone networks. As a result of these arguments and concerns from the telecommunications industry,[1] as well as issues raised by groups advocating protection of privacy rights,[2] the Communications Assistance for Law Enforcement Act (CALEA) was enacted on October 25, 1994 (47 USC 1001-1021), in the final days of the 103rd Congress.

CALEA is intended to preserve the ability of law enforcement officials to conduct electronic surveillance effectively and efficiently, despite the deployment of new digital technologies and wireless services by the telecommunications industry. CALEA requires telecommunications carriers to modify their equipment, facilities, and services to ensure that they are able to comply with authorized electronic surveillance. These modifications were originally planned to be completed by October 25, 1998. To date, however, implementation of CALEA is significantly behind schedule because the telecommunications industry, law enforcement agencies, and privacy rights groups have not reached an agreement on technical issues. Issues also remain concerning the amount of federal funds to be provided to the telecommunications carriers for implementation of CALEA, and the privacy rights of individuals that may be affected under various implementation scenarios.

Some Technical Terms

As a result of the revolution in digital technology in telecommunications, the process of wiretapping and other electronic surveillance has become more complex,

---

[1] In this report, the telecommunications industry includes common carrier telephone companies, mobile wireless telecommunications providers, telecommunications equipment manufacturers, and other entities that provide telecommunications services to the public.

[2] Privacy rights groups involved in the CALEA debate include the Electronic Privacy Information Center, the Electronic Frontier Foundation, advocacy groups which both support on-line privacy rights of individuals, the Center for Democracy and Technology, which also advocates electronic privacy (and is funded primarily by the telecommunications, computer, and media industries), and the American Civil Liberties Union (ACLU), which represents a broad array of civil rights based on the First and Fourth Amendments.

and legal ambiguities have been introduced. As a background to understanding the problems associated with CALEA implementation, the definitions of several terms are necessary. Electronic surveillance refers to either the interception of communications content (as in a conversation) also known as *wiretapping*, or the acquisition of call-identifying information (the number dialed). The latter activity is accomplished through the use of *pen register devices*, which capture call-identifying information for numbers of outgoing calls from the location of lawful interception, and *traps and traces*, which capture information for numbers received at the location of lawful interception, much like consumer caller ID systems. Under current federal law, law enforcement (i.e., police or the FBI) must obtain a court order before conducting any of these activities. However, a wiretap requires a higher "evidentiary burden" than a pen register or trap and trace, including showing that there is probable cause for believing that a person is committing one of a list of specific crimes.[3]

Under traditional analog technology, it was easy to separate the above categories of electronic surveillance. However, the advent of digital signal transmission technologies has made that distinction less clear. Information signals (voice or data) can be transmitted over telephone networks in one of two ways: *circuit-switched* and *packet-switched* modes.[4] In circuit-switched systems, a communications path is established between the parties and dedicated exclusively to one conversation for the duration of the call. In packet-switched systems, the information is broken down into smaller pieces called "packets"using a digital process. Each packet contains a small part of the message content along with call-identifying information called a "header" that indicates the origination and destination points of the information. Each packet is transmitted separately and is reassembled into the complete message at the destination point.

The packet-switched mode is the signal transmission technology used in all Internet communications. Packet switching is considered a more efficient use of a network than circuit switching because the same line can be used for multiple communications simultaneously. Although the circuit-switched mode was historically used in all voice telephone calls, the packet-switched mode is increasingly being used for voice and data transmissions over telephone networks.

CALEA's Main Provisions

CALEA requires telecommunications carriers to assist law enforcement in performing electronic surveillance on their digital networks pursuant to court order or other lawful authorization. The telecommunications industry, privacy rights groups, and law enforcement agencies agree that CALEA was not intended to expand law enforcement's authority to conduct electronic surveillance. On the contrary,

---

[3]See CRS Report 98-326 A, *Taps, Bugs & Telephony: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, March 23, 1998.

[4]Switches are network devices that select a path or circuit for sending data to its next destination over the telephone network. Switches may also include functions of the router, a device also used in computer networks, that determines the route and adjacent network point for data to be sent.

CALEA was intended only to ensure that after law enforcement obtains the appropriate legal authority, carriers will have the necessary capabilities and sufficient capacity to assist law enforcement in conducting digital electronic surveillance regardless of the specific telecommunications systems or services deployed.

CALEA (47 USC 1002) directs the telecommunications industry to design, develop, and deploy solutions that meet certain assistance capability requirements for telecommunications carriers to support law enforcement in the conduct of lawfully-authorized electronic surveillance. Pursuant to a court order or other lawful authorization, carriers must be able, within certain limitations, 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 that is reasonably available on 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.

To allow carriers to give law enforcement the means to conduct its wiretaps, CALEA (47 USC 1003) requires the Attorney General to determine the number of simultaneous interceptions (law enforcement agencies' estimate of their *maximum capacity* requirements) that telecommunications carriers must be able to support. This action was originally required within one year of enactment, but was later delayed (see **Initial Delays** below).

To maintain privacy rights of individuals, CALEA (47 USC 1004) requires telecommunications carriers to ensure that any interception of communications or access to call-identifying information that is conducted within their premises can only be done with a court order. It also requires the specific intervention of an officer or employee of the carrier acting in accordance with regulations prescribed by the Federal Communications Commission (FCC).

CALEA (47 USC 1005) directs telecommunications carriers to consult with telecommunications equipment manufacturers to develop equipment necessary to comply with the capability and capacity requirements identified by the FBI. For efficient industry-wide implementation of the above requirements, CALEA (47 USC 1006) directs the law enforcement community to coordinate with the telecommunications industry and state utility commissions to develop suitable technical standards and establish compliance dates for equipment. The FCC may grant extensions to the compliance dates if it determines that the capability requirements are not reasonably achievable within the compliance period.

CALEA (47 USC 1008) gives the Attorney General, subject to the availability of appropriations, authority to pay telecommunications carriers for all reasonable costs directly associated with the modifications performed by carriers in connection with equipment, facilities, and services installed or deployed on or before January 1, 1995 (known as the "grandfather" date).

Major Events Following Enactment of CALEA

Initial Delays

CALEA gave implementation responsibility to the Attorney General, who, in turn, delegated the responsibility to the FBI. The FBI leads that nationwide effort on behalf of federal, state, and local law enforcement agencies. FBI officials initially anticipated that it would take a year for a standard to be developed and agreed upon by law enforcement, the telecommunications carriers, and the equipment manufacturers. Telecommunications consultants estimated that it would take the industry another three years to design, build and deploy new systems to comply with CALEA. Instead, industry and law enforcement became involved in a protracted dispute over what should be required for law enforcement's wiretapping capabilities.

By March 1997, the completion of the capability standard was overdue by 16 months. The FBI attempted to expedite the industry's implementation of CALEA by releasing regulations that included a cost recovery plan for the federal government's payment of costs associated with CALEA, as well as capability and capacity requirements for the industry to meet. The plan required more extensive upgrades to networks than the telecommunications industry believed were necessary for law enforcement to preserve its wiretapping capabilities. Industry groups and privacy advocates disputed the FBI's plan. They argued that the FBI was attempting to expand its surveillance capabilities beyond the congressional intention of CALEA, and was attempting to unfairly shift costs and accountability away from the federal government onto private industry. Furthermore, the industry argued that, without an adopted capability standard, it could not begin designing, manufacturing, and purchasing the equipment to achieve CALEA compliance.

In December 1997, the Telecommunications Industry Association (TIA, representing telecommunications equipment manufacturers) adopted, over the objections of the law enforcement community, a technical standard, J-STD-025, also known as the "J-standard." This standard prescribes upgrades to network devices to meet CALEA's assistance capability requirements for local exchange, cellular, and broadband personal communications services (PCS). Although the FBI claimed that the J-standard did not provide all of the capabilities needed, the industry asserted that CALEA's language stated that telecommunications carriers would be compliant if they met publicly available standards adopted by the industry.

Privacy rights groups, on the other hand, protested two aspects of the J-standard that they asserted would make information beyond what is legally required available to law enforcement. One was a feature enabling the telecommunications network to provide location information for users of mobile wireless telecommunications services. The location information protocols in J-STD-025 allow law enforcement agencies to obtain information on the physical location of the nearest cell site (i.e., the receiver/transmitter antenna and base station) of mobile phone handsets at the beginning and end of each call. Wireless carriers are now deploying another technology (called triangulation) that will enable the carriers, and law enforcement, to track wireless telephone users more precisely, potentially within a few meters. The other was a feature enabling the network to access packet-mode data from telephone

calls using more advanced systems. Privacy rights groups argued that these capabilities would violate the Fourth Amendment rights of individuals against unreasonable searches and seizures. Despite these objections, telecommunications manufacturers began designing new switches and upgrades to existing switches according to the J-standard.

The FBI's "Punch List"

In the negotiations in developing the J-standard, TIA had refused to include some of the capabilities that law enforcement officials wanted to facilitate digital wiretapping. As a result, in March 1998, the FBI petitioned the FCC to require the telecommunications industry to adopt those additional capabilities. Industry and privacy rights groups protested that the FBI's plan would unlawfully expand enforcement capabilities. Labeled the "punch-list" by the telecommunications industry (because of its perceived attempt to force the industry to comply), the plan included the capabilities to:

(1) intercept the content of conference calls initiated by the subject under surveillance (including the call content of parties on hold) pursuant to a court order or other legal authorization;
(2) obtain information during conference calls identifying all active parties to the call, and whether a party has been put on hold, has joined, or has been disconnected from the call;
(3) monitor when the subject under surveillance uses "vertical services" such as call-forwarding and call-waiting;
(4) retrieve call timing information, i.e., when calls are initiated and completed;
(5) obtain "dialed digital extraction" capability that shows any digits on the handset pressed by a surveillance subject after a call has been connected, including credit card or bank account numbers;
(6) monitor "surveillance status," requiring carriers to send information to law enforcement agencies to verify that a wiretap had been established;
(7) monitor "continuity check tone," requiring that a dial tone be present on the channel received by law enforcement until the surveillance subject uses the phone;
(8) monitor when a surveillance subject adds or deletes any communications services;
(9) monitor "in-band and out-of-band signaling," requiring carriers to send a notification message to law enforcement when the network sends signals to the subject's phone, such as special rings, busy signals, and call-waiting signals.

Capacity Requirements

The FBI's subsequent implementation actions were also opposed by the telecommunications industry. In March 1998, the FBI announced its estimated capacity requirements for local exchange, cellular, and broadband personal

communications services (PCS).[5] The industry protested the FBI's estimates, arguing that it would require telephone carriers to accommodate thousands of wiretaps simultaneously, an impractical and unnecessary burden. In July 1998, the FBI developed guidelines and procedures to facilitate small carrier compliance with its capacity requirements, and asked carriers to identify any systems or services that did not have the capacity to accommodate those requirements. In December 1998, the FBI began a proceeding to develop capacity requirements for services other than local exchange, cellular, and broadband PCS, asked additional questions of interested parties in June 2000.[6] These technologies and services included paging, mobile satellite services, specialized mobile radio, and enhanced specialized mobile radio. To date, that proceeding has not been completed.

FCC Actions

As a result of petitions from the industry and the FBI, the FCC became involved in the implementation of CALEA. In October 1997, the FCC released its first Notice of Proposed Rule Making (NPRM) on CALEA implementation.[7] The NPRM sought comments from interested parties regarding a set of policies and procedures proposed by the FCC for telecommunications carriers to follow. The proposed procedures would (1) preclude the unlawful interception of communications, (2) ensure that authorized interceptions are performed, (3) maintain secure and adequate records of any interceptions, and (4) determine what entities should be subject to these requirements, whether the requirements are reasonable, and whether to grant extensions of time for compliance with the requirements. The telecommunications carriers, privacy rights groups, and the FBI all submitted comments to the FCC to attempt to influence the final decision.

In April 1998, the FCC released a Public Notice requesting comments on issues raised in petitions from industry, the FBI, and privacy rights groups concerning the dates that carriers were required to comply with CALEA and the dispute over the J-standard. Based on comments it received, the FCC extended the deadline until June 30, 2000 for telecommunications carriers to comply with CALEA, stating that without a standard, the necessary equipment would not be available in time.[8]

In October 1998, the FCC initiated a proceeding to review the technical capabilities prescribed by the J-standard.[9] The goal of that proceeding was to determine whether telecommunications carriers should be required under CALEA to meet the FBI's "punch list" items. The FCC addressed these issues in several

---

[5]Federal Register 63, page 12217, FBI, Final Notice of Capacity, March 12, 1998.

[6]Federal Register 63, page 70160, FBI Notice of Inquiry, December 18, 1998, and page Federal Register 65, page 40694, FBI Further Notice of Inquiry, June 30, 2000.

[7]FCC NPRM CC Docket No. 97-213, FCC Record 97-356, released October 10, 1997.

[8]FCC Memorandum Opinion and Order in the Matter of Petition for the Extension of the Compliance Date under Section 107 of CALEA, released September 11, 1998.

[9]FCC Proposes Rules to Meet Technical Requirements of CALEA. Report No. ET 98-8. FCC News, October 22, 1998.

documents released over the following year. In March 1999, the FCC's First Report and Order established the minimum capability requirements for telecommunications carriers to comply with CALEA.[10] Telecommunications carriers were required to ensure that only lawful wiretaps occur on their premises and that the occurrence of wiretaps is not divulged to anyone other than authorized law enforcement personnel. On August 2, 1999, the FCC decided to allow carriers to decide how long they would maintain their records of law enforcement's wiretap, pen register, and trap and trace interceptions.[11] On August 31, 1999, the Second Report and Order established a definition for "telecommunications carrier" to include all common carriers, cable operators, electric and other utilities that offer telecommunications services to the public, commercial mobile radio services, and service resellers.[12] The definition did not include Internet service providers (ISPs), which were explicitly excluded under the CALEA statute.

The FCC's Third Report and Order, released August 31, 1999, adopted technical requirements for wireline, cellular, and broadband PCS carriers to comply with CALEA requirements.[13] The ruling adopted the J-standard, including the two capabilities that were opposed by the privacy rights groups (i.e., the ability to provide location information and packet-mode data to law enforcement). The FCC also adopted six of the nine punch list capabilities requested by the FBI to be implemented by telecommunications carriers (punch list items 6, 7, and 8 listed above were not granted). The Order required all aspects of the J-standard except for the packet-mode data collection capability to be implemented by June 30, 2000. The Order required carriers to comply with the packet-mode data capability and the six punch list capabilities by September 30, 2001. Some privacy rights groups expressed outrage over the ruling, stating that the FCC had "threatened civil liberties and may even grant the FBI new powers of surveillance." Upon adoption of the ruling, however, FCC Chairman William Kennard stated that "We have carefully balanced law enforcement's needs against the rights of all Americans to privacy, and the cost to industry of providing these tools to assist law enforcement."[14]

Issues for Congress Regarding CALEA

Despite the contention among all of the parties involved, issues associated with the implementation of CALEA have not been given a great amount of attention in Congress. While funding for CALEA has been discussed at appropriations hearings, the only oversight hearing focusing specifically on CALEA implementation was by the House Judiciary Committee, Subcommittee on Crime, on October 23, 1997. Furthermore, to date, no reports have been published by the General Accounting

---

[10]FCC 99-11, Report and Order CC Docket No. 97-213, released March 15, 1999.

[11]FCC 99-184, Order on Reconsideration CC Docket No. 97-213, released August 2, 1999.

[12]FCC 99-229, Second Report and Order, CC Docket No. 97-213, released August 31, 1999.

[13]FCC 99-230, Third Report and Order, CC Docket No. 97-213, released August 31, 1999.

[14]FCC Sides with FBI on Tapping, *Wired News*, August 27, 1999. [http://www.wired.com/news]

Office or the Congressional Budget Office on CALEA implementation issues. However, several issues have not been resolved, and deadlines for implementation have passed while others are approaching.

Funding

While cost estimates for CALEA implementation continued to rise after its enactment, funding was slow to come. CALEA authorized $500 million to be distributed to telecommunications carriers for implementation. Shortly after enactment, the U.S. Telecommunications Association (USTA), representing over 1,200 large and small telephone companies called the local exchange carriers (LECs), estimated the cost at $2 billion. By 1999, some industry estimates placed CALEA costs at $5 billion. The Department of Justice (DOJ) has disputed the higher estimate. However, the Attorney General did acknowledge that "In excess of $2 billion would be needed by the government to reimburse telecommunications carriers to cover the costs of modifying this enhanced embedded base."[15]

No funding, however, was appropriated for CALEA for three years after enactment. The Omnibus Consolidated Appropriations Act of 1997 (P.L. 104-208) created the Telecommunications Carrier Compliance Fund (TCCF) for CALEA implementation. The 1997 Act provided $60 million to DOJ for CALEA implementation, which could not be released until the implementation plan was approved by House and Senate Appropriations Committees. The 1997 Act also authorized agencies with law enforcement and intelligence responsibilities to transfer unobligated balances into the TCCF.

The FY1998 Appropriations Act for Commerce, Justice, State Departments and Related Agencies (P.L. 105-119), did not provide additional funding to the TCCF. The accompanying conference report (H. Rept.105-405) stated that there was already $101 million in the Fund "which is sufficient to support reimbursement to the telecommunications industry during FY1998."[16] The FY1999 Omnibus Appropriations Act (P.L.105-277) also did not provide any new funding, although a small amount of interest accrued to the Fund, and transfers were made from other federal agency accounts, bringing the total to $102.5 million. DOJ received an additional $15 million in FY2000 appropriations for CALEA implementation.

For FY2001, the Administration's budget request included $120 million to be distributed by DOJ and another $120 million to be distributed by the Department of Defense (DOD) for CALEA implementation.[17] The FY2001 Commerce, Justice,

---

[15]Letter from Attorney General Janet Reno to Honorable Ted Stevens, Chairman of Senate Committee on Appropriations, October 6, 1998.

[16]Telecommunications Carrier Compliance Fund, *Congressional Record*, November 13, 1997, page H10836.

[17]Budget of the United States Government FY2001, Appendix, page 631, submitted February 7, 2000. The rationale behind providing some of the funds to DOD, to be redistributed to DOJ, was that law enforcement often assists DOD in conducting wiretaps on suspected

(continued...)

State Appropriations Act (P.L. 106-553) provided another $201 million for the TCCF.[18] In addition, a large portion of the TCCF appropriations was inserted into the FY2001 Military Construction Appropriations Act (P.L. 106-246). This law was enacted on July 13, 2000, under a section providing supplemental appropriations for FY2000 "for an additional amount for 'Salaries and Expenses', $181 million to remain available until expended, which shall be deposited in the TCCF," under the Drug Enforcement Administration supplemental appropriations. In total, Congress has appropriated $499,557,270 for the TCCF. As of January 15, 2001, the unobligated balance of the TCCF is $227,757,270, although no money has yet been provided to the carriers. The Administration is expected to request significant additional TCCF funding for FY2002.

In addition, the FBI's costs for CALEA implementation have been criticized by telecommunications industry groups as being exorbitant. The FY2001 Commerce, Justice, State Appropriations Act (P.L. 106-553) provides $17.3 million for the FBI's CALEA implementation activities. FY2000 appropriations for the FBI's CALEA implementation was $15 million to remain available until expended. The FBI declined to provide any information on its funding or expenditures for CALEA implementation.

Equipment and Standards

The industry standard (J-STD-025) with added "punch list" items adopted by the FCC in August 1999, defined services and features to support electronic surveillance by law enforcement agencies. The J-standard includes interfaces to provide law enforcement agencies access to packet-mode data and location information. Privacy rights groups criticize this provision, claiming that it essentially creates a situation in which mobile telephones can be converted into location-tracking devices. They argue that neither the packet-mode data, nor the location information, are authorized by CALEA, and that these capabilities violate the Fourth Amendment rights of individuals against unreasonable searches and seizures.

Both the DOJ and the FBI expressed satisfaction with the FCC's requirements for carriers, even though the FCC did not include three of the FBI's "punch list" items in its decision. Attorney General Janet Reno stated that "This ruling will enable law enforcement to keep pace with these changes [in telecommunications technology] and ensure we will be able to maintain our capability to conduct court-authorized electronic surveillance."[19] Some observers questioned whether the three deleted "punch list" items were ever necessary for law enforcement's crime fighting purposes.

---

[17](...continued)
international criminals, in which case the FBI's CALEA capabilities could be used for national security purposes.

[18] All of this amount is provided under DOJ appropriations even though $141.3 million of it is designated for national security purposes.

[19]Justice Department press release regarding the FCC's CALEA standards, August 27, 1999.

Privacy rights groups questioned whether any of the punch list capabilities were necessary for law enforcement to conduct wiretaps in the future.

Many carriers were not able to meet the FCC's June 30, 2000 deadline for upgrading their systems to be compliant with the J-STD-025 (required for all carriers by the FCC's Third Report and Order). Of the approximately 3,600 telecommunications carriers in the Untied States (including wireless, wireline, cable, and international carriers), about 2,000 of them did not meet the deadline. Many of them petitioned the FCC for an extension, arguing that CALEA-compliant equipment and software had not become available as extensively as had been expected.[20] The FCC granted an extension to some petitioners until March 31, 2001, and is reviewing other petitions on a case by case basis. In the majority of petitions, carriers claim they will become CALEA-compliant by 2002.

The next CALEA deadline for carriers to meet is March 12, 2001, as defined by the FBI (63 Fed. Reg. 12217, March 12, 1998), when carriers providing local exchange, cellular services, and broadband PCS must comply with the capacity requirements. This entails additional hardware and software upgrades for all switches operated by carriers to enable (multiple, in some cases) electronic surveillance actions at any given time. The FBI determined a separate capacity requirement for each county in the United States. The telecommunications industry disputed the number of wiretaps the FBI required carriers to support, arguing that law enforcement has never before asked for a wiretap at many of the locations indicated. The FCC decided that capacity requirements fall outside of its jurisdiction, and has not become involved in the dispute between carriers and the FBI on that issue. Many carriers have petitioned the FBI for an extension of that deadline, based on the lack of availability of equipment and the lack of resources to make the upgrades.

By September 30, 2001, wireline, cellular, and broadband PCS carriers are required to implement the additional "punch list" capabilities adopted by the FCC. On August 23, 2000, the Cellular Telecommunications Industry Association filed a petition for a waiver of that deadline for its cellular and PCS provider members.[21] Other carriers may also petition for an extension to that deadline. On September 29, 2000, TIA submitted a report to the FCC on the technology and privacy issues involved in applying CALEA to packet-mode services.[22] As a result of that study, TIA recommended that the FCC to suspend the compliance date for packet-mode communications requirements, based on the uncertainty for equipment manufacturers and carriers in knowing how to satisfy CALEA requirements following a recent court decision (Privacy Issues Associated with CALEA, below) that questioned the legal requirements for law enforcement agencies to monitor packet-mode communications.

---

[20]FCC *Public Notice*, rpt. no. CALEA-001, CALEA Section 107(c) Extension Petitions Filed, released June 30, 2000.

[21]For a copy of the filing, see [http://www.wow-com.com/lawpol/filing/pdf/ctia082300.pdf]

[22]Report to the FCC on Surveillance of Packet-mode Technologies, September 29, 2000. http://www.tiaonline.org/government/filings/JEM_Rpt_Final_092900.pdf.

Impact on the Telecommunications Industry

The FBI estimated that about 3,600 telecommunications companies defined as "carriers" by the FCC's Second Report and Order are required to upgrade their systems for CALEA-compliance. These include local exchange carriers, interexchange carriers, competitive access providers (also called service resellers), wireless service providers, satellite communications companies, and any other company that offers telecommunications services to the public. Since few cable television companies, electric and other utilities currently offer telecommunications services to the public, those industries are not significantly affected.

To facilitate CALEA implementation, in March 2000 the FBI established a "Flexible Deployment Assistance" program, through which carriers could file for an extension to a CALEA deadline.[23] To be considered for an extension by the FCC, carriers are required to submit detailed information to the FBI on the types of equipment they had deployed.[24] Because the FCC made this information a prerequisite to the granting of an extension, the FBI collected the information primarily from carriers that filed for an extension.[25] The FBI plans to determine which equipment within the higher priority jurisdictions (identified by state and local law enforcement agencies) must have CALEA upgrades installed first. Only the equipment in the lower priority areas will be granted extensions. It is not clear when the FBI will release its list of priority areas.

Under the CALEA statute, carriers will not be reimbursed for CALEA upgrades to network devices that were deployed or installed after January 1, 1995. All of the PCS infrastructure (which was deployed after January 1995), and most of the infrastructure of the cellular industry (some of which was in place prior to 1995) is exempt from reimbursement under CALEA. CALEA further states that equipment installed prior to January 1, 1995 does not have to be upgraded unless the FBI decides that it is necessary and pays all of the costs of the upgrade. Carriers will be responsible, however, to make and pay for CALEA upgrades to equipment that has had "significant" upgrades since January 1995. Most equipment in the wireline telephone infrastructure has had some level of upgrades (e.g., corrections for the year 2000 computer problem). That fact has caused many in industry to speculate that much of the costs for CALEA upgrades on equipment deployed even before 1995 will have to be paid by industry.[26] Many other commercial mobile radio services such as enhanced paging, specialized mobile radio, multichannel multipoint distribution

---

[23]The FBI's "Flexible Deployment Assistance Guide" containing questions for carriers to answer in order to file for an extension to a CALEA deadline, can be found at CTIA's website at [http://www.wow-com.com/lawpol/guide.cfm].

[24]The FCC has regulatory authority to grant extensions to telecommunications carriers, but under CALEA, it must consult with the Attorney General before granting an extension.

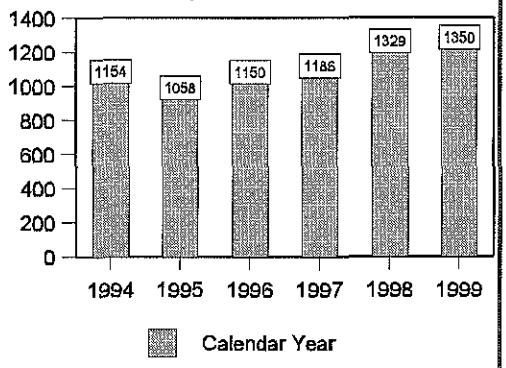
[25]Some carriers unknowingly provided the information requested in the Flexible Deployment Assistance Guide and sent it to the FBI without needing to file for an extension.

[26]According to one estimate, 30-50% of the wireline industry will have to make and pay for CALEA upgrades.

service, and local multipoint distribution service, must also make and pay for upgrades to their systems.

Any costs not reimbursed by the TCCF could ultimately be passed on to consumers. Some argue that CALEA has created an incentive for telecommunications carriers not to make any general upgrades to their networks due to concerns that the FBI will deem the upgrades to be "significant" and deny reimbursement for CALEA upgrades. Also, some claim that as a result of FBI interference with the business plans of telecommunications firms, U.S. companies have been hindered in their business transactions with foreign companies.

Figure 1: Total Federal and State Wiretap Authorizations



Source: Report of the Director of the Administrative Office of the U.S. Courts on Applications for Orders Authorizing Interception of Wire, Oral, or Electronic Communications, published April 2000

Is CALEA Necessary? Is it Effective?

Given that CALEA has still not been implemented over six years after enactment, some question whether it was ever necessary. Privacy rights groups argue that there is insufficient evidence that law enforcement has been hampered without the new capabilities to be provided by CALEA. As shown in Figure 1, the number of authorized state and federal wiretaps has increased an average of three percent per year since CALEA's enactment, to a total of 1,350 such actions in 1999. During this period, all but three requests for wiretaps were authorized by the courts. Surveillance of new technologies (such as those provided by wireless or other advanced services) accounted for over half of all requests. Privacy rights groups point to that data to argue that the advent of digital telephone networks has not impeded law enforcement from performing wiretaps, counter to what has been argued by the FBI. Others might argue, however, that crimes have gone undetected as a result of the lack of CALEA upgrades.

Some question whether CALEA can ultimately solve law enforcement's problem of being able to perform wiretaps in a digital telecommunications environment. Given the extensive delays in implementing CALEA and the extensions granted to many telecommunications carriers, some question whether the industry, law enforcement, and privacy rights differences will ever be resolved, or whether the FCC's decisions will ever be upheld by the courts. Even if all telecommunications carriers finally become fully CALEA-compliant, some believe that in the future, strong encryption will be used often enough in telecommunications (both voice and data) that law enforcement will be unable to decipher the content of communications that it

collects.[27] Some question whether the goal of CALEA to preserve law enforcement's wiretapping capabilities in the digital age, equal to those capabilities under traditional analog telecommunications systems, is still realistic.

Privacy Issues Associated with CALEA

Privacy rights groups are concerned that the FBI, in its implementation actions, is trying to usurp greater capabilities than were intended by CALEA. They claim that the FCC's interpretation of CALEA has endangered the public's right to privacy by permitting law enforcement to obtain the actual content of conversations over telecommunications networks, instead of only the call origination information (e.g., the number dialed), in violation of the Fourth Amendment.

Some telecommunications industry groups claim that the FBI's Flexible Deployment Assistance program violated the privacy rights of telecommunications carriers by requiring them to submit detailed information on their networks in order to be considered for an extension to the June 30, 2000, deadline of CALEA implementation. The FCC did not provide guidance to carriers until April 25 on how to file for extensions to the June 30 deadline, thus, carriers contended, giving them little time to dispute the FBI's procedures.[28] Telecommunications industry representatives argue that the FBI can now use the proprietary information provided by the carriers to deny reimbursement for future CALEA upgrades.

In January 2000, some privacy rights groups, together with telecommunications industry groups, filed suit with a federal appeals court to block the FBI's requirements placed on carriers and on mobile telecommunications devices.[29] The lawsuit was based on arguments over privacy rights, disputes over the equipment standards adopted by the FCC, the FBI's capacity requirements, and the FBI's procedures for making payments to the carriers for upgrades. On August 15, 2000, the court upheld some aspects of the J-standard, while overturning other aspects.[30] The court decided that the FCC correctly required carriers to build into their systems a capability to provide location information on wireless phones, but that the requirement is limited to the antenna handling the call at the time of interception. The court also ruled that government agents must meet the highest legal standards if they want to intercept packet-mode data from telephone signal transmissions. The court further ruled that the FCC exceeded its statutory authority granted by CALEA in its

---

[27]Will Crypto Feast on Carnivore? *Wired News*, August 4, 2000 [http://www.wired.com/news/0,1294,37915,00.html].

[28]FCC *Public Notice* 00-154, CALEA Section 103 Compliance and Section 107(c) Petitions. April 25, 2000.

[29]Three law suits were originally filed with the U.S. Court of Appeals for the DC Circuit against the FCC's August 1999 rulings. The Court consolidated the three petitions into a single petition which can be found at [http://www.epic.org/privacy/wiretap/].

[30]U.S. Telecom Association et al., Petitioners v. Federal Communications Commission and United States of America, Respondents AirTouch Communications Inc., et al., Intervenors. See [http://pacer.cadc.uscourts.gov/common/opionions/200008/99-1442a.txt] for the court ruling.

adoption of four of the six punch list capabilities adopted by the FCC, and remanded consideration of those requirements back to the FCC.[31] The FCC is currently considering alternatives for how to satisfy the court's concerns.[32]

The Internet Dimension: The FBI's Carnivore System

Since personal and business communications are being conducted increasingly over the Internet (in both e-mail and Worldwide Web transactions), the law enforcement community has become interested in being able to conduct wiretapping over that medium. In 1999, the FBI asked the Internet Engineering Task Force (IETF), an industry-led standards-setting body for Internet protocols, to consider adopting protocols for wiretapping for use by Internet service providers. Several individuals and groups protested this suggestion. They argued that this development would harm network security, result in an increase in illegal activities, diminish users' privacy, stifle innovation, and impose significant costs on developers of communications equipment and services. In November 1999, the IETF decided overwhelmingly to reject the FBI's proposal.

On February 28, 2000, at a joint hearing of the House Judiciary Crime Subcommittee and the Senate Judiciary Oversight Subcommittee, the DOJ and the FBI argued that having the authority to conduct wiretaps over the Internet would help law enforcement in investigating cyber-attacks. Unbeknown to the public (or to the White House, according to some reports), however, the FBI had already developed a special software program, called "Carnivore," to efficiently collect Internet communications. The Carnivore system includes a "network analyzer" or "sniffer" that collects information from e-mail and other Internet communications.[33] A separate device that runs the Carnivore program is installed at each Internet Service Provider (ISP) to sort through the incoming and outgoing traffic at the ISP to find information flowing to and from a person under investigation. Prior to activating these systems, the FBI obtains court orders for a pen register/trap and trace surveillance. The FBI does not use Carnivore for many of the larger ISPs, which maintain in-house capabilities to enable law enforcement's Internet monitoring. There are, however, probably thousands of ISPs that do not have that capability.

The existence of Carnivore was discussed at a hearing on July 24, 2000, held by the House Judiciary Committee, Subcommittee on the Constitution. Some witnesses at the hearing were concerned that the Carnivore system could enable the collection of the content of communications, equivalent to a wiretap (which requires a higher burden for law enforcement to show that a crime is likely being committed). The FBI

---

[31]The four punch list capabilities that were remanded to the FCC are items 2, 4, 5, and 9 in the list provided above.

[32]FCC *Public Notice* DA 00-2342, Commission Seeks Comments to Update the Record in the CALEA Technical Capabilities Proceeding CC Docket No. 97-213, October 17, 2000.

[33]A sniffer is a common program used by network administrators to analyze the flow of communications "traffic," detect bottlenecks and keep traffic flowing efficiently.

claimed that only information or messages of relevance to a court-approved criminal investigation are stored and reviewed, and other information is discarded. Privacy and civil rights groups question whether anything prevents other non-approved communications from being collected.

Privacy Issues Associated With Internet Monitoring

Many have seen a parallel between the privacy issues raised in the implementation of CALEA and those associated with monitoring Internet communications. Some suspect that the FBI is trying to avoid the pitfalls it encountered in implementing CALEA in its efforts to intercept Internet traffic. They argue that the FBI may be trying to convince the computer industry to adopt a single standard for Internet monitoring technology. Then, as Internet communications grow, the FBI could monitor Internet traffic more efficiently. On April 6, 2000, the House Judiciary Committee, Subcommittee on the Constitution, held a hearing on the Fourth Amendment and the Internet. Several witnesses at the hearing warned of the lack of legal protections for the privacy of Internet communications, while one witness believed that the existing laws governing privacy on the Internet were adequate.[34]

It is technically possible for the FBI to use systems such as Carnivore to collect the content of communications of individuals who have not been served a court order, in violation of the Fourth Amendment. Some call for placing a greater burden on the ISPs to protect the privacy of communications to which government access has not been granted. Others argue that once a system such as Carnivore is installed, the ISP has little control over what information the FBI accesses, and therefore should be immune from prosecution. Legal issues related to Internet monitoring are becoming increasingly urgent as the technical tools for online surveillance (and the ability to thwart those activities) improve and proliferate.

In addition, two relatively new services might present privacy rights issues in connection with CALEA implementation and Internet monitoring. These services are Internet access over mobile telephones and the placement of phone calls via the Internet.[35] Each of these services raises the question of whether they should be regulated as Internet or telephone communications, and over what privacy protections they should be granted. As various communications technologies (including the telephone, the Internet, digital television, and various wireless systems) continue to converge, the application of regulations and laws governing their separate uses has become an issue of potential congressional interest.

The Attorney General agreed to conduct an in-house review of Carnivore, but declined to release the system's source code or design to the public, citing the potential for revealing its weaknesses. On August 2, 2000, a federal judge ordered the FBI to expedite its review of a request made by privacy rights groups for the

---

[34]Testimony from the House Judiciary Committee, Subcommittee on the Constitution, hearing April 6, 2000.

[35]Internet telephony, also called voice over Internet protocol (VoIP), is the transmission of voice traffic as data packets over a packet-switched data network instead of as a synchronous stream of binary data over a conventional circuit-switched voice network.

immediate release of details on the technology and capabilities of Carnivore. On August 16, in response to a court order the FBI announced that it would review 3,000 pages of documents pertaining to Carnivore to determine what can be released under the Freedom of Information Act (FOIA), and release information in increments every 45 days. Privacy rights groups objected to the FBI's caveat that some of the information might be redacted (i.e., edited or revised prior to release) based on FOIA exemptions covering national security, privacy, and other concerns. On October 2, 2000, the FBI released the first set of documents from its files on Carnivore, most of which was redacted or completely withheld.

On September 6, 2000, the Senate Judiciary Committee held a hearing on the Carnivore controversy. At the hearing, FBI officials testified that over the past two years they had used the system about 25 times, and only with the permission of the courts. A witness from the Center for Democracy and Technology, a privacy rights group supported in part by the telecommunications industry, argued that the potential for government abuse is high and suggested that the Internet Service Providers should control the operations of the Carnivore system. Senator Hatch, the Committee Chairman, and another witness, Dr. Vinton Cerf, founding president of the Internet Society, raised questions about whether private sector corporations can be trusted any more than the government.[36]

In response to the congressional inquiries and media reports, the Attorney General agreed to an "independent technical review" of Carnivore. Several leading academic institutions declined to bid on the DOJ's proposal, however, due to concerns that the DOJ reserved the right to edit or omit sections of the report.[37] On September 26, the DOJ selected the Illinois Institute of Technology Research Institute (IITRI) to review the system. Its report, released on November 21, concluded that Carnivore functions as the FBI had described, and generally does not "over-collect" information. The report also stated, however, that "While the system was designed to, and can, perform fine-tuned searches, it is also capable of broad sweeps. Incorrectly configured, Carnivore can record any traffic it monitors." The report further stated that "IITRI did not find adequate provisions (e.g., audit trails) for establishing individual accountability for actions taken during use of Carnivore."[38] The report also made recommendations for improving Carnivore for efficiency and protecting the privacy of Internet users.

On November 21, 2000, the Chairman and Ranking Member of the Senate Judiciary Committee asked the FBI to "explain why Carnivore was tested to determine if it was capable of intercepting and archiving unfiltered traffic though ana ISP, whether Carnivore in fact has that capability, and under what circumstances it could ever be legitimately used to draw on that capability." They also requested "complete and unredacted copies of the documents produced in response to the FOIA

---

[36]Senate Judiciary Committee hearing, September 6, 2000. Federal News Service Transcript.

[37]"Universities Unwilling to Review FBI's 'Carnivore' System," [http://www.CNN.com/2000/TECH/computing/09/06/carnivore/index.html].

[38]IITRI Independent Technical Review of the Carnivore System, Draft Report, 17 November, 2000. [http://www.usdoj.gov/jmd/publications/carniv_entry.htm].

lawsuit together with any other documents related to Carnivore's capability to intercept and archive unfiltered traffic."

Given the increase in Internet communications and the increase in law enforcement's electronic surveillance activities, the FBI is likely to increase its use of Carnivore systems in its Internet monitoring efforts. In addition, the September 2000 TIA report to the FCC on surveillance of packet-mode technologies, suggested using Carnivore technology for telephone wiretaps as a way of meeting CALEA requirements and maintaining a separation between content and packet information.[39] Many industry observers argue that the merging of technologies used for telephone and Internet communications has necessitated a change in law to establish a parity of procedures for digital surveillance by law enforcement.

Relevant Legislation in the 106th Congress

Several bills were introduced in the 106th Congress concerning electronic surveillance. On April 21, 1999, the Electronic Rights in the 21st Century Act was introduced (S. 854, Leahy). The bill is intended to protect the privacy of the electronic communications of individuals by increasing the requirements for a warrant or subpoena before the government could obtain the electronic communications contents or location information from a service provider, among other provisions. While not affecting CALEA implementation directly, the bill would increase the burden on law enforcement in obtaining a court order, and could reduce the number of wiretaps performed. The bill was referred to the Senate Judiciary Committee and no further action was taken.

The Notice of Electronic Monitoring Act (H.R. 4908, Canady, introduced July 20, 2000) would have required employers to notify their employees when they monitor e-mail communications and other computer usage in the workplace (companion bill, S. 2898, Shumer, introduced July 20). The bills were referred to the House and Senate Judiciary Committees, respectively, with no further action taken.

Two bills intended to limit law enforcement's electronic surveillance activities were introduced on July 27, 2000. The Digital Privacy Act of 2000 (H.R. 4987, Barr) would have increased the reporting requirements for the Attorney General on the electronic surveillance activities of the DOJ. The bill would also increase limits on government access to contents of stored electronic communications (including e-mail) and to location information of mobile electronic devices. The Electronic Communications Privacy Act of 2000 (H.R. 5018, Representative Canady) would also increase the Attorney General's reporting requirements on the electronic surveillance activities of the DOJ, and excludes electronic communications (both stored and real-time), if seized without proper authority, from being used as evidence in court or agency hearings. H.R. 5018 originally did not include a section on limiting

---

[39] *FCC Could Adopt Carnivore*, Wired News, September 29, 2000.

government access to content of stored electronic communications (later added in an amendment), and includes other specific differences from H.R. 4987.[40]

The House Judiciary Committee, Subcommittee on the Constitution, held a hearing on September 6, 2000, on H.R. 4908, H.R. 4987, and H.R. 5018. Privacy rights groups and industry representatives supported most aspects of the three bills. The DOJ expressed concern that this legislation could interfere with law enforcement's ability to conduct digital surveillance. On September 14, H.R. 5018 was adopted by the Subcommittee on the Constitution, with an amendment added from part of H.R. 4987 to limit government access to location information of mobile electronic devices. The House Judiciary Committee approved H.R. 5018 (amended) on September 26 (H.Rept. 106-932 released October 4, 2000). No further action was taken on either of these bills.

[40]For a detailed description of H.R. 5018, see CRS Report RS20693 by Gina Marie Stevens.