BADM 590: IT Governance

The CALEA Effect

Andrew Maxedon

5/2/2007
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.</td>
<td>Abstract</td>
<td>Pg 3</td>
</tr>
<tr>
<td>1.</td>
<td>Introduction</td>
<td>Pg 3</td>
</tr>
<tr>
<td>2.</td>
<td>Review</td>
<td>Pg 3-6</td>
</tr>
<tr>
<td>2.1</td>
<td>CALEA Act</td>
<td>Pg 3-4</td>
</tr>
<tr>
<td>2.2</td>
<td>The First and Second Orders</td>
<td>Pg 4-5</td>
</tr>
<tr>
<td>2.3</td>
<td>Concerns</td>
<td>Pg 5</td>
</tr>
<tr>
<td>2.4</td>
<td>Additional Information</td>
<td>Pg 6</td>
</tr>
<tr>
<td>3.</td>
<td>Case Study</td>
<td>Pg 6</td>
</tr>
<tr>
<td>3.1</td>
<td>Introduction</td>
<td>Pg 6</td>
</tr>
<tr>
<td>3.2</td>
<td>History</td>
<td>Pg 6</td>
</tr>
<tr>
<td>3.3</td>
<td>The Problem</td>
<td>Pg 6</td>
</tr>
<tr>
<td>3.4</td>
<td>The Solution</td>
<td>Pg 7</td>
</tr>
<tr>
<td>3.5</td>
<td>Summary</td>
<td>Pg 7-8</td>
</tr>
<tr>
<td>4.</td>
<td>Solutions</td>
<td>Pg 8</td>
</tr>
<tr>
<td>4.1</td>
<td>Current Status</td>
<td>Pg 8</td>
</tr>
<tr>
<td>4.2</td>
<td>Solera Networks</td>
<td>Pg 8-9</td>
</tr>
<tr>
<td>4.3</td>
<td>Apogee</td>
<td>Pg 9-10</td>
</tr>
<tr>
<td>4.4</td>
<td>Solutions Summary</td>
<td>Pg 11</td>
</tr>
<tr>
<td>5.</td>
<td>Costs</td>
<td>Pg 11-12</td>
</tr>
<tr>
<td>6.</td>
<td>Discussion</td>
<td>Pg 12-13</td>
</tr>
<tr>
<td>7.</td>
<td>Conclusion</td>
<td>Pg 13</td>
</tr>
</tbody>
</table>

Appendix A: Solera Control Center _______Pg 14  
Appendix B: Excerpt from CALEA___________Pg 15-18  
References______________________________Pg 19
Abstract

As of May 14, 2007, legally recognized public telecommunications carriers in the United States will be required to keep records of all transactions across their networks. This act entitled Communications Assistance for Law Enforcement Act, or CALEA, has added to the costs telecommunications carriers incur but is necessary with the increasing amount of information transmitted over digital and analog services. CALEA not only provides the opportunity for law enforcement but also businesses to monitor network traffic for their own purposes, assuming ownership of that data. In this paper, CALEA will be briefly described, the history of the act and some early monitoring technologies, some costs involved in the implementation and technical options carriers have in order to meet requirements in a timely fashion.

1. Introduction

This project will focus on some of the technical options and controls available that allow carriers to comply with CALEA. These technologies are significant not only from a compliance standpoint but also from a business standpoint. With this technology, businesses will not only be able to comply with CALEA more cost effectively, but will be able to audit information sent over their networks. We will also analyze some of the reasons for CALEA and the impact it can have on the public. Near the end of the case, a brief overview of analytic search software will be discussed to compliment the CALEA research.

2. Review

2.1 CALEA Act

The Communications Assistance for Law Enforcement Act (CALEA) was passed on October 25, 1994 in response to the FBI’s concern that the future use of digital telephone equipment would make wire tapping phones more difficult and more time consuming. At the time, since compliance required phone companies to modify their existing equipment and include CALEA compliant interfaces, the
U.S. Congress provided some funding over a limited period of time to cover these costs. The original CALEA order was put into affect on January 1, 1995.

2.2 The First and Second Orders

In March of 2004, the department of justice, FBI and DEA filed a petition which requested certain steps be taken to ensure and accelerate compliance with CALEA. The FCC subsequently issued a notice of proposed rulemaking and received public comment which resulted in the adoption of the “First Report and Order.” This order specified that CALEA applied to broadband internet access facilities and providers of Voice-over-Internet-Protocol (VoIP) services. Further public comment resulted in the commission investigating exemptions from CALEA’s requirements. In May 2006, the FCC adopted the “Second Report and Order.” This second order clarified the first order and affirmed it with set dates.

The following outlines the main points of these orders:

- CALEA compliance deadline is May 14, 2007 and applies to all interconnected VoIP service providers in addition to broadband based access providers. There are restricted compliance extensions available.

- Service providers affected by the First Order must be in compliance with the security requirements of the First Order within 90 days of the Second Order taking affect.

- Carriers are solely responsible for the development of CALEA and implementation costs associated with CALEA. Carriers may not recover said costs by issuing any type of national surcharge.
• Carriers are permitted to comply with CALEA through a “Trusted Third Party (TTP).” This includes everything from processing intercept requests to delivering information to law enforcement agencies. Carriers still remain responsible for ensuring the information be presented in a timely manner in addition to the protection of subscriber privacy.

2.3 Concerns

These are the main points of the orders and were put in to effect in an effort to ensure CALEA compliance with every medium of communication publicly used. Some standards organizations have adopted standards to ensure compliance with CALEA. One example is the American National Standard for Telecommunications (ATIS). They have published a standard for broadband intercept. There are currently some arguments, mainly from the VoIP community, being announced against CALEA and some of the security and design concerns for VoIP. The following is a quote by the Information Technology Association of America (ITAA) on VoIP and CALEA compliance:

“In order to extend authorized interception much beyond the easy scenario, it is necessary either to eliminate the flexibility that Internet communications allow, or else introduce serious security risks to domestic VoIP implementations. The former would have significant negative effects on U.S. ability to innovate, while the latter is simply dangerous. The current FBI and FCC direction on CALEA applied to VoIP carries great risks.”
2.4 Additional information
Just like seatbelts in cars made before seatbelts were invented, circuit switching equipment that was made prior to January 1, 1995 is not required to be CALEA compliant. However, if that equipment is significantly upgraded, CALEA compliance is again required. Unfortunately, this exemption does not apply to packet switching equipment as intercepts can be put in place separately from the actual packet switch.

3. Case Study
3.1 Introduction
Recently VeriSign, a major trusted third party in CALEA services, published a case study on the Vonage VoIP network.

3.2 History
Vonage is a New Jersey based provider of broadband telephone services. They have over 2 million subscriber lines and have in excess of 5 billion network calls annually. Vonage allows a customer to place a phone call virtually anywhere a broadband connection exists, providing they have their Vonage handset, etc.

3.3 The Problem
However, Vonage’s network must interface with traditional phone systems to provide traffic termination to the customer. Vonage had to decide between the installation of its own switching network or outsourcing. A switching center would require a significant capital outlay and increased time to service.
3.4 The Solution

Vonage elected to outsource and chose VeriSign’s SS7 services. SS7 stands for Signaling System 7 and is a set of protocols used to initiate most of the world’s public switched telephone network (PSTN) calls. VeriSign operates the largest independent SS7 network worldwide. Due to the complexity of VeriSign’s operation, it was able to offer additional services to Vonage such as full compliance with CALEA. Vonage was not required to comply with CALEA at the time but, with forethought, decided to choose a solution that could handle future CALEA requests. The following is an excerpt from the case:

“A typical CALEA compliant deployment demands significant investments in dedicated hardware, staff training, and process execution. The VeriSign NetDiscovery Services help minimize these requirements through the use of a single connection to the VeriSign network. The VeriSign suite of services is the premier turnkey solution for provisioning, access, delivery, and collection of call information from operators and providers to law enforcement agencies. Holder stated, ‘We will be able to attain continuous, hassle-free compliance with CALEA, as well as benefiting from a considerable reduction in the complexity and cost of our CALEA implementation.’”

3.5 Summary

There were several challenges for Vonage to overcome. First, Vonage had to locate a cost effective and credible solution enabling them to outsource certain components of their infrastructure. Another challenge was to find a partner who
was reliable and had a good record, credibility, and speed. One final challenge was for Vonage to find a way to reduce the complexity and expense involved in deployment with ongoing operations. The solution was to use VeriSign Connectivity and Interoperability Services (SS7) Connectivity and VeriSign NetDiscovery Services. This allows Vonage to be fully compliant in the future and take advantage of the suite of CALEA services VeriSign can deliver.

4. Solutions

4.1 Current Status

There are several current solutions being sold to help carriers comply with CALEA. Most of the solutions belong to trusted third parties but some are sold solely as equipment for the carrier to add to existing networks.

4.2 Solera Networks

Solera networks sells a device called the 1U Solera CALEA Appliance which is used by the carrier as a CALEA data collection and security device. This device has many features and can capture data at OC12 data rates with an onboard storage capacity of 800 GB. It can be deployed through a network TAP or SPAN port on the existing network which allows for invisible packet capture. The following are some of the advantages of the included CALEA appliance software:

- Provides LEA collector capability
- Support CMII Packet annotation and forwarding
- Provides full 7X24 packet capture with dynamic TAP filtering capability
- Provides TAP forwarding of captured data to LEAs
- Can provide historical views of network traffic
As can be seen, this device is very capable of facilitating CALEA compliance. However, the cost is around $6,995 per unit. Depending on the amount of data and data transfer rates of the carrier, there may be a requirement for multiple or more complex units. This could lead to higher costs, especially with the amount of data being exchanged daily growing exponentially in the near future. Of course, such an appliance can be used for nearly any type of logging as it enables full-length recording of network activity. An example of the Solera interface can be found in Appendix A.

4.3 Apogee

Apogee provides a slightly different solution which is more of a service than a device. It is called the Secure Intercept Service, or SIS. It provides complete compliance for interception, administration, and delivery standards of CALEA. It’s often more cost-effective for smaller networks to use this approach rather than an in-house solution. This solution is provided in four steps:

1. Access the intercepted data
2. Administer the intercept
3. Convert the intercepted data into delivery standard
4. Securely deliver intercepted data to LEA systems
This solution supports most network schemes and can support custom schemes as well. The following is a diagram illustrating how this system works:

As is shown, this method requires little to no additional hardware purchase and can be managed without additional personnel. There are several advantages to this approach for smaller organizations:

1. Minimizes operating expenses
2. Keeps compliance costs predictable
3. Frees up valuable IT resources
4. Secure data exchange
5. Customizable to current network
6. Preserved network security
7. Adaptability to emerging technology

Apogee is just one of several solutions available.
4.4 Solutions Summary

As shown by the two examples above, there are several different methods with which to comply. These are just two of the more popular examples but additional options exist.

5. Costs

Costs for CALEA compliance vary greatly with the size of the organization and the requirements in both hardware and services to comply. For some rural telephone companies, experts report a startup cost of as much as $150,000. Most of the larger telecom companies, such as Verizon and AT&T, are already in compliance. Even though the startup costs seem steep, the fines by the FCC may be worse. Currently, fines of $10,000 per day are being threatened for non-compliance if there is a warrant for lawful intercept that cannot be executed. For UIUC, Mike Corn, Security and Privacy Director stated it could cost UIUC around $30 million to be in compliance if it were considered a public provider. Below is a chart with examples of costs from startup to annual:

<table>
<thead>
<tr>
<th>Cost of CALEA</th>
<th>Just in time</th>
<th>Trusted third party</th>
<th>In-house solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approximate one-time cost of solution</td>
<td>$10,000 for minimum configuration, depends on number of intercepts and number of carrier switches</td>
<td>Up to $30,000, depends on number of intercepts and number of carrier switches</td>
<td>$70,000 to $150,000 baseline price, suitable for 15,000 subscriber systems</td>
</tr>
<tr>
<td>Approximate yearly cost of solution</td>
<td>~10% of equipment cost (e.g., ~$1200)</td>
<td>~10% of equipment cost (e.g., ~$5000 to $10,000)</td>
<td>Depends on number of carriers switches and design of carrier network</td>
</tr>
</tbody>
</table>

Source: The Balcer Horbat Law Group
Obviously compliance is required but costly depending on the size of the organization. The ability this gives the carrier, however, can have a great affect on business processes.

6. Discussion

Of course, a business executive can find a use for just about any government requirement. For instance, SOX regulations have facilitated the implementation of controls on not only accounting but information technology as well. These controls are enacted through standards, such as COBIT; much like CALEA has standards. This brings us to the business use of CALEA. Since CALEA requires the ability to intercept and log all network traffic, this allows companies to utilize this ability in other ways than just compliance. There are some legal issues to be considered but, for the most part, as long as a company owns the network; it owns the traffic. For instance, if a company were to log all network traffic and would need to investigate an email that has since been deleted from the servers, it could look over the logs and retrieve the email transmission. Since CALEA compliance requires real-time recording of network activity, any transmission can be rebuilt just as it happened.

Of course this is just one example of how such technology could be used. Another example is from a troubleshooting standpoint. Often, an error occurs in a network application or in an internet based program and it is hard to track exactly what the user did over the network to create the problem. With this logging system in place, it would be more efficient in analyzing network activity and determining the root cause of the problem instead of just making
assumptions and the “fixed it for now” approach. As is demonstrated by these and countless other uses, CALEA can have returns on investment for companies in addition to avoiding penalties by the FCC and law enforcement agencies. Of course, with all of this data, there is the process of translating it into information and knowledge. This is where I would like to discuss an interesting company called RiverGlass which makes analytic search engine software to sort through all the data and return only pertinent information. The search engine technology sorts through all of the data, in this case packets, for certain keywords and, using statistical modeling, determines the relevance of each packet so the user is only presented with the most accurate and relevant data based on their specifications. There are other software programs that do this as well. The purpose in this discussion is to demonstrate the need for a way to turn the data into knowledge if companies decide to use the CALEA compliance in their favor.

7. Conclusion

Overall, CALEA is a simple rule which requires very complex methods to be in compliance with. This paper is just a simple overview of what CALEA is, how it can be implemented, and some of the costs/benefits of the implementation. Overall, I believe CALEA is just another example of how the world is moving away from the mentality of making it work towards more controls and efficiencies in information technology which will facilitate better and more scaleable systems and networks for the future. Appendix B contains an excerpt of the legal code of CALEA.
Appendix A: Solera Appliance Control Center
Appendix B: Excerpt from CALEA

Communications Assistance for Law Enforcement Act of 1994

One Hundred Third Congress
of the
United States of America

AT THE SECOND SESSION

An Act

To amend title 18, United States Code, to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, and for other purposes.

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

TITLE I--INTERCEPTION OF DIGITAL AND OTHER COMMUNICATIONS

SEC. 101. SHORT TITLE.

This title may be cited as the `Communications Assistance for Law Enforcement Act'.

SEC. 102. DEFINITIONS.

For purposes of this title--

(1) The terms defined in section 2510 of title 18, United States Code, have, respectively, the meanings stated in that section.

(2) The term `call-identifying information' means dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier.

(3) The term `Commission' means the Federal Communications Commission.

(4) The term `electronic messaging services' means software-based services that enable the sharing of data, images, sound, writing, or other information among computing devices controlled by the senders or recipients of the messages.

(5) The term `government' means the government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory, or possession of the United States, and any State or political subdivision thereof authorized by law to conduct electronic surveillance.

(6) The term `information services'--
Appendix B: Excerpt from CALEA (cont.)

(A) means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications; and

(B) includes--

(i) a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities;
(ii) electronic publishing; and
(iii) electronic messaging services; but

(C) does not include any capability for a telecommunications carrier's internal management, control, or operation of its telecommunications network.

(7) The term `telecommunications support services' means a product, software, or service used by a telecommunications carrier for the internal signaling or switching functions of its telecommunications network.

(8) The term `telecommunications carrier'--

(A) means a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire; and

(B) includes--

(i) a person or entity engaged in providing commercial mobile service (as defined in section 332(d) of the Communications Act of 1934 (47 U.S.C. 332(d))); or
(ii) a person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of this title; but

(C) does not include--

(i) persons or entities insofar as they are engaged in providing information services; and
(ii) any class or category of telecommunications carriers that the Commission exempts by rule after consultation with the Attorney General.

SEC. 103. ASSISTANCE CAPABILITY REQUIREMENTS.

(a) CAPABILITY REQUIREMENTS- Except as provided in subsections (b), (c), and (d) of this section and sections 108(a) and 109(b) and (d), a telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of--

(1) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government;
Appendix B: Excerpt from CALEA (cont.)

(2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier--

(A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and
(B) in a manner that allows it to be associated with the communication to which it pertains, except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18, United States Code), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number);

(3) delivering intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier; and

(4) facilitating authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects--

(A) the privacy and security of communications and call-identifying information not authorized to be intercepted; and
(B) information regarding the government's interception of communications and access to call-identifying information.

(b) LIMITATIONS-

(1) DESIGN OF FEATURES AND SYSTEMS CONFIGURATIONS- This title does not authorize any law enforcement agency or officer--

(A) to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services; or
(B) to prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services.

(2) INFORMATION SERVICES; PRIVATE NETWORKS AND INTERCONNECTION SERVICES AND FACILITIES- The requirements of subsection (a) do not apply to--

(A) information services; or
(B) equipment, facilities, or services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers.

(3) ENCRYPTION- A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.
Appendix B: Excerpt from CALEA (cont.)

(c) EMERGENCY OR EXIGENT CIRCUMSTANCES- In emergency or exigent circumstances (including those described in sections 2518 (7) or (11)(b) and 3125 of title 18, United States Code, and section 1805(e) of title 50 of such Code), a carrier at its discretion may comply with subsection (a)(3) by allowing monitoring at its premises if that is the only means of accomplishing the interception or access.

(d) MOBILE SERVICE ASSISTANCE REQUIREMENTS- A telecommunications carrier that is a provider of commercial mobile service (as defined in section 332(d) of the Communications Act of 1934) offering a feature or service that allows subscribers to redirect, hand off, or assign their wire or electronic communications to another service area or another service provider or to utilize facilities in another service area or of another service provider shall ensure that, when the carrier that had been providing assistance for the interception of wire or electronic communications or access to call-identifying information pursuant to a court order or lawful authorization no longer has access to the content of such communications or call-identifying information within the service area in which interception has been occurring as a result of the subscriber’s use of such a feature or service, information is made available to the government (before, during, or immediately after the transfer of such communications) identifying the provider of a wire or electronic communication service that has acquired access to the communications.

SEC. 104. NOTICES OF CAPACITY REQUIREMENTS.

(a) NOTICES OF MAXIMUM AND ACTUAL CAPACITY REQUIREMENTS-

(1) IN GENERAL- Not later than 1 year after the date of enactment of this title, after consulting with State and local law enforcement agencies, telecommunications carriers, providers of telecommunications support services, and manufacturers of telecommunications equipment, and after notice and comment, the Attorney General shall publish in the Federal Register and provide to appropriate telecommunications industry associations and standard-setting organizations--

(A) notice of the actual number of communication interceptions, pen registers, and trap and trace devices, representing a portion of the maximum capacity set forth under subparagraph (B), that the Attorney General estimates that government agencies authorized to conduct electronic surveillance may conduct and use simultaneously by the date that is 4 years after the date of enactment of this title; and

(B) notice of the maximum capacity required to accommodate all of the communication interceptions, pen registers, and trap and trace devices that the Attorney General estimates that government agencies authorized to conduct electronic surveillance may conduct and use simultaneously after the date that is 4 years after the date of enactment of this title.

(2) BASIS OF NOTICES- The notices issued under paragraph (1)--

(A) may be based upon the type of equipment, type of service, number of subscribers, type or size or carrier, nature of service area, or any other measure; and

(B) shall identify, to the maximum extent practicable, the capacity required at specific geographic locations.
References:


[2] FCC, Communications Assistance For Law Enforcement, AskCALEA. Available at: http://www.askcalea.net/


[4] FCC, FCC ADOPTSS ORDER TO ENABLE LAW ENFORCEMENT TO ACCESS CERTAIN BROADBAND AND VoIP PROVIDERS. Available at: http://www.askcalea.net/docs/20060503_2nd-memorandum.pdf


