

GLOBAL LAWFUL INTERCEPTION INDUSTRY FORUM WHITE PAPER

SECURITY IMPLICATIONS IN  
APPLYING THE  
COMMUNICATIONS ASSISTANCE  
FOR LAW ENFORCEMENT ACT  
AND RELATED REQUIREMENTS  
TO VOICE OVER IP

---

**1 INTRODUCTION**

---

This paper was prepared by the industry association<sup>1</sup> of companies that implement and support lawful interception (LI) technical capability requirements worldwide which includes CALEA – the U.S. *Communications Assistance for Law Enforcement Act of 1994*. The material provided here attempts to provide a balanced treatment of the needs and challenges of implementing real-time access to VoIP signalling and content under CALEA, and how these needs are mandated via public communication infrastructure requirements throughout the world. The paper also describes the work among industry and government ongoing in many active diverse cooperative activities and actions.

The many parties who are part of this global collaborative lawful interception activity fully understand the technologies involved, the associated challenges, and the costs. The policies reached and the mandates imposed, have typically followed years of industry collaborative activity and public policy making proceedings in numerous local, national and international legislative, regulatory, and judicial forums – in which technological alternative views have been extensively articulated and then rejected, accepted or balanced.

Over the past decade, well-meaning technical experts have occasionally banded together and launched critical campaigns against CALEA, including related laws imposing national security, consumer, and infrastructure protection requirements. With only minimal understanding of the actual legal and forensic requirements, such critics have typically produced dismissive pronouncements and papers asserting broad brush

---

<sup>1</sup> The Global Lawful Interception Industry Forum is the principal industry organization among providers of products, services, and expertise worldwide that develop and implement the law enforcement forensic support capabilities for communications systems in nearly every nation and pursuant to international agreements. See [www.gliif.org](http://www.gliif.org)

incompatibilities with contemporary network technologies, dismissing existing public policy and industry forums, and asserting unspecified “risks.”<sup>2</sup>

The real “risks,” however, are the delays in implementing significant, trusted forensic capabilities for VoIP and other IP-Enabled services that include CALEA. The species of cybercrime are multiplying as fast as the legitimate applications, and often scaling faster than number of users. This doesn’t even include non-economic crime such as protection against the terrorists, drug cartels, pedophiles, and other organizations and individuals with criminal intent.

Forensic detection, analysis, and capture capabilities for these kinds of activities are needed no matter what the technology. TCP/IP is just another protocol – not some mystical charm that wards off all evil. The continued refusal of uninformed CALEA critics to participate in or accept the decisions of expert decision making agencies like the FCC or FBI, or engage in work in technical forums organized by industry is unfortunate.

The security implications arising from not implementing needed VoIP forensic capabilities are substantial. Applying CALEA requirements to VoIP enhances security of the public communications infrastructure, together with its providers and users, rather than diminishing it. The requirements also enhance privacy.

---

## 2 HOW CALEA WORKS

---

CALEA was enacted by the U.S. Congress in 1994 expressly for the purpose of providing “future proof” capabilities for law enforcement agencies to obtain real-time forensic evidence when a criminal suspect uses public electronic communication networks and services. In the U.S., as it was worldwide, the increasing difficulties faced by these agencies in obtaining critically needed evidence, was rapidly being eroded by new digital and internet technologies. The result in both the U.S. and many other countries was a statutory requirement for law enforcement to promulgate a few basic technology neutral “capability requirements.”

In the U.S. the legislative instrument was entitled CALEA. What was somewhat unique about CALEA was that the industry itself – even individual providers - could then implement the requirements as they chose. The FBI developed the capability requirements. Service providers and equipment vendors were encouraged to develop “safe harbor” standards to reduce costs through common platforms, but ultimately the responsibility was imposed on individual service providers. The FCC was authorized to play the role of arbitrator when disputes arose, as well as the implementation enforcing agency.

The CALEA requirement itself is a simple and essential one that has endured throughout the history of public communications – a service provider must provide technical and operational capabilities to extract evidence available to the provider when a customer is shown likely to be engaging in criminal conduct. The mandate is essential because there are simply no alternatives. Such assistance capabilities are important to

---

<sup>2</sup> The classic reference statement in this regard is Internet Engineering Task Force (IETF) RFC2804, *IETF Policy on Wiretapping*, May 2000, refusing to engage in lawful interception work. Recently, a more recent variant has been produced. See, e.g., Bellovin et al, *Security Implications of Applying the Communications Assistance to [sic] Law Enforcement Act to Voice over IP*, May 21, 2006.

providers to avoid civil or criminal liabilities, and to both providers and customers to enhance the trust and integrity of the public communication services infrastructure. The security policy requirements of CALEA also enhance privacy and the integrity of the judicial process. Today's open and dynamic public communication infrastructures produce substantial vulnerabilities while effectively incenting large-scale fraud, cyberstalking, terrorism, and predatory behavior. CALEA is designed to help mitigate these unfortunate results.

### COMMON CALEA “URBAN LEGENDS”

Particularly among insular technical communities and CALEA critics, many legal and public policy misconceptions are asserted as fact. Some of the most common are listed here.

- **CALEA is a uniquely U.S. requirement.** In fact, CALEA-like provisions exist in almost every country and region in the world and are generally far more extensive, detailed, and vigorously enforced than in the U.S. Unlike the U.S. which has an “information services” exception, every other country requires full compliance for all publicly available services. These CALEA equivalent capabilities are coordinated and treated by many different intergovernmental and industry forums. Global cooperation on technical standards principally occurs through the European Telecommunication Standards Institute Technical Committee on Lawful Interception.
- **The principal interested party is the FBI.** The majority of lawful interceptions in the U.S. are done by the more than 10,000 state and local law enforcement offices under local law. Under CALEA, the Attorney General is responsible for coordinating and representing all law enforcement and delegates certain responsibilities to the FBI. This model is similar to most “Ministries of Justice” in countries worldwide. Because CALEA concerns the production of evidence to prosecute crimes (especially those which occur on-line), as well as the protection of network infrastructure and the domestic pursuit of terrorism and espionage, it is the network service providers and the American public who are the ultimate interested parties.
- **CALEA makes the infrastructure wiretap ready.** CALEA, in fact, has a very limited and focused objective – enabling the hand over of basic real-time forensic data and content by a service provider when a court has determined a customer may be engaging in criminal conduct, and that data or content is reasonably available on the provider's facilities. CALEA itself states this objective in very generic terms – quickly isolating and enabling the interception of call signalling and communications of a specific subscriber which is available to the provider by virtue of providing the equipment and service. It is worth noting that most providers today already implement forensic acquisition capabilities similar or even more extensive than those sought by law enforcement - to protect criminal behavior directed against their own network infrastructure and services.

- **CALEA changes the “design process.”** CALEA, in fact, expressly does not change the design process. The forensic capability requirements of law enforcement are stated in generic terms, and each provider is free to support those requirements in any reasonable manner. There are a substantial number of options available to providers – ranging from changes to specific equipment or systems to “overlay” solutions that are minimally intrusive. Numerous industry collaborative forums also exist to help sort through these options and develop common “safe harbor” solutions. Trusted Third Party service bureaus provide turnkey solutions tailored to a provider’s infrastructure design. Ultimately it is the service provider’s choice as to the means employed.
- **CALEA requires standards.** Under CALEA in the U.S., no standards are specified to implement a compliance solution – only generic requirements. This approach was chosen by Congress and underscored in FCC decisions to allow providers the flexibility to pursue their own solutions. This policy approach is covered at some length in the FCC *Second Order* released on 12 May. In most other countries, specific lawful interception standards are mandated and enforced through both regulatory and regular administrative testing practices. This is not the case in the U.S. where the CALEA approach provides greater flexibility and minimizes effects on infrastructure design and evolution.
- **CALEA adversely affects innovation.** Because the CALEA approach does not rely on any specific compliance standards, providers are actually required to “innovate” CALEA solutions as they develop new platforms and services. In the *FCC Second Order*, it was also made clear that no “pre-approval” requirement would be established under CALEA. No credible argument exists for an assertion that CALEA affects innovation.
- **CALEA will force service providers to move abroad.** Perhaps the most preposterous CALEA urban legend is the “service providers will move abroad” assertion. Most significant nations have requirements that are at least as extensive as CALEA. While some very remote jurisdictions may indeed exist that do not have lawful interception requirements, it is unlikely that this will compel any serious business to move to avoid the obligations, and in any case, the domestic service providers interconnecting with such a foreign provider would still be subject to the requirements.
- **CALEA is expensive.** The expense of meeting CALEA requirements for all but the very smallest providers lies largely in obtaining the necessary mediation equipment and maintaining a security office. Fortunately, these expenses are miniscule in a large provider organization, and for smaller companies can be shared in a Trusted Third Party arrangement. The costs are always going to be significantly reduced using such arrangements. In the FCC’s CALEA proceeding, a consultant calculated the TTP costs for significant size providers at less than a penny per subscriber per month – which have been confirmed in practice.
- **Roving wiretaps make CALEA worthless.** Some argue that nomadic usage patterns using combinations of wireless and IP-based network

technologies make CALEA worthless. In fact, it is such nomadic usage and the resulting roving wiretaps that have been facilitated under the Patriot Act that have made CALEA so essential.

- **CALEA endangers privacy.** The statutory requirements that have been implemented by the FCC require providers to established designated contacts for implementing judicial orders, implementation policies, audit trails, and security practices designed to enhance subscriber privacy, not diminish it.

## CURRENT CALEA INTERNET AND VoIP REQUIREMENTS

Under a pair of regulatory orders adopted by the FCC after more than three years of countless workshops, thousands of filed comments, and enormous industry collaborative activity, certain requirements must be met by most Internet service providers. Those providers who offer to the public either facilities-based broadband Internet access service or Interconnected VoIP Services (i.e., interconnected with the public telephone network) must establish a security office and procedures for supporting law enforcement, and notify related information to the FCC by late October 2006. The same providers must also by May 2007 implement the ability to extract the communications signalling information and content of a specific subscriber – to the extent they can reasonably do so. Providers can either implement these capabilities themselves or they can outsource the requirements to existing Trusted Third Party service bureaus. Industry standards and equipment are available. Internet providers worldwide have long been subject to even more extensive requirements in most countries.

Some parties sought to challenge the FCC Orders by obtaining review in a Federal appeals court just below the U.S. Supreme Court. The court conducted the review and held in early June that the FCC's requirements were reasonable as the nation's expert agency for dealing with the nation's public communication systems.

---

### 3 MORE THAN JUST CALEA

---

The opponents of CALEA capabilities for VoIP/Internet tend to ignore that bases other than the CALEA statute exist for the requirements. One particularly obvious recent example is the enactment by Congress of new law that defines Internet software – especially VoIP related software – to constitute a telecommunications device for the purposes of enforcing anti-cyberstalking provisions under the Violence Against Women Act. Congress clearly intended technology neutral capabilities be implemented by providers to assist in minimizing Internet based crime. Indeed, the requirements to identify a user are almost identical to a similar requirement in CALEA.

The CALEA criticism also ignores the reality that most providers and equipment vendors themselves implement CALEA equivalent capabilities to facilitate network operations, to mitigate against fraud, and to investigate network attacks and failures. It was no surprise that the leading Internet equipment vendors simply adapted existing network management systems software to implement CALEA Internet capabilities for their provider customers.

---

## 4 HOW THE PSTN AND VOIP ARE THE SAME UNDER CALEA

---

CALEA Internet critics frequently justify their views arguing that the public telecommunications networks and “the Internet” are somehow fundamentally different so as to preclude the implementation of CALEA requirements or otherwise justify a safety zone for criminals and terrorists. In actuality there are little or no differences between the technology platforms today. The public telecommunication/telephone networks in the 1980s move to packet network platforms for the subscriber communications channels and internet-like platforms for the signalling. Indeed, the telecommunication infrastructure is designed to be more robust and protected to meet national critical infrastructure and other public policy requirements.

“The Internet” simply emulates these same capabilities using home-grown protocols that are either proprietary or developed by Internet developer forums. This inherent functional similarity is one of the reasons why many countries long ago rejected the argument that “the Internet is different” for the purposes of meeting lawful interception obligations. CALEA itself is technology neutral. The requirement obliges a provider must “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” isolating and delivering intercepted communications and call-identifying information to the government “that is reasonably available” to the provider.

The “reasonably available” provision is particularly important whether the platform is the PSTN or VoIP. If the subscriber communications or call-identifying information is not reasonably accessible to the carrier, the capabilities are not obligated under CALEA.

---

## 5 HOW SECURITY IS ENHANCED UNDER CALEA

---

On many different levels and by different measures, security and privacy are significantly enhanced under CALEA. Perhaps the foremost security enhancement is enjoyed by the subscribers using the communications network – knowing that other users engaging in criminal conduct ranging from fraud and drug dealing to child predators and kidnappers can be effectively investigated and prosecuted for their conduct via the network. Network providers themselves enjoy similar security enhancements in being able to better protect their network facilities and systems against hackers by enabling their investigation and prosecution by law enforcement.

The principal reason why CALEA and its equivalent lawful interception capabilities have been imposed worldwide – whether for VoIP or any other application - is because it is necessary. When someone has been kidnapped; when pedophiles are stalking children; when drug dealers or terrorists or all manner of criminals conspire or prey on a victim – it is often necessary to acquire real-time evidence. There are no other choices. This means wiretapping, and increasingly with today’s widespread interoperable IP-Enabled networks combined with nomadic users and applications, this means CALEA capabilities. It is not possible anymore to have government Geek Squads running around trying to attach their own equipment.

CALEA's customer identification, network security, security office, and new "proof of performance" requirements also significantly add to the technical, operational, and administrative capabilities of providers. This additional set of security capabilities – whether instituted by the provider or a Trusted Third Party – improves network security and end user privacy at both local and national levels.

The alternative to CALEA – which is to effectively create a free haven for criminal behavior and hacking – is untenable by any measure. It is the antithesis of security.

---

## 6 WHY INNOVATION IS NOT A CONCERN IN APPLYING CALEA TO VOIP

---

CALEA critics often impute dire consequences to network innovation and subscriber use if CALEA requirements are imposed on VoIP providers. An especially amusing USA-centric admonition is the assertion that providers and innovators will simply leave U.S. shores as a result of CALEA. What the critics ignore is that relative ease and minimal cost by which the capabilities can be implemented, as well as the reality that countries worldwide have similar if not more extensive law enforcement support requirements.

In fact, the deficient lack of CALEA Internet and VoIP requirements compared to the rest of the world that has long imposed them, has resulted in a global network forensics and analysis marketplace where some of the most innovative vendors in that market exist outside the U.S. The more imposing requirements outside the U.S. is also reflected in the work of the European Telecommunication Standards Institute as the principal venue for innovative global lawful interception specifications.

---

## 7 SUMMING UP

---

CALEA critics today are pushing the same stale arguments for the past decade – all of which have no merit – and rejected time and again in industry, policy making, and judicial venues. In most cases, the arguments manifest little or no understanding of the law, the regulations, the industry standards, or the implementations involved. Most importantly, the advocacy ignores the very real needs of users, providers, and society for these capabilities worldwide. The "not our problem" attitude of CALEA critics provides no remedies.

It is now time to move forward and implement the CALEA requirements now mandated by the FCC and sustained by the courts to meet needs that are plainly evident. The "real risk" of not implementing CALEA for VoIP is, in fact, the security of the American public. This is protection against the threats of terrorists, drug cartels, pedophiles, and other organizations and individuals with criminal intents. This protection must be provided regardless of technology.

In the U.S., compared to other countries, CALEA regulations have in some ways shifted the burden unfairly from VoIP application providers to broadband ISPs to implement VoIP forensic capabilities. This shift occurred when the Commission moved away from the "managed/mediated" criterion for responsibility applied in most other countries. If VoIP or any other application service providers manage or mediate services to subscribers/users, they should be required to comply with CALEA regardless of their

mediation location or interconnection with the PSTN. The VoIP provider should be responsible for intercepting bad guys using their service between two IP phones it is mediating, not the poor ISP that is only providing Internet access and derives no benefit from the VoIP provider's service.

Lack of technology for supporting CALEA never has been an issue. Even in VoIP, nearly all calls (99%) are managed using centralized softswitches, SIP servers or Skype-like supernodes. With this control, calls (the voice content) can be routed through network elements capable of interception. The only VoIP interception responsibility which cannot be imposed on a VoIP provider is where two users with public IP addresses establish a call on a true peer-peer basis. In this case, the broadband ISP must be responsible for interception.

As some LI system vendors have noted at recent industry events, the challenge of peer-to-peer communications will require new techniques and technology to assure that forensic information can be obtained – which in turn should be reflected in CALEA requirements. This has been characterized as a shift from a “VoIP LI for ISP-centric approach to a LI for peer-to-peer IM. This also involves a shift from an “identifier centric” approach to “parametric signature” techniques. Industry and government are already collaborating on solutions.

Lawful interception in the U.S. should be treated less as a law enforcement assistance measure under CALEA, and more as a forensics measure for infrastructure protection and national security need under Title I. The approach also avoids CALEA's outmoded “information services” exception. The especially important forensic measure of Data Retention has already been adopted and is now being implemented in Europe and countries in other regions while some critics in the U.S. are still arguing over lawful interception.

Lawful interception was able to move forward in the past few years largely because of the Sept 11 disaster. Public Safety E911 requirements for VoIP were implemented because of accumulating numbers of personal tragedies. The Data Retention Directive was moved toward adoption by a series of transportation bombings where the value of retained data proved decisive in capturing the perpetrators. This kind of reactive security approach in regulatory policy making tends to ensure that future disasters of some kind – whether purposeful or accidental - will occur before network based remedial action is taken. Without proactive regulation for national security and public safety, the “bad guys” with the incentives and know-how will gravitate to technology and services where they have a safe haven.