Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Communications Assistance for	)	ET Docket No. 04-295
Law Enforcement Act and	)	
Broadband Access and Services	)	RM-10865

Reply Comments of VeriSign, Inc.

Anthony M. Rutkowski
Vice President for Regulatory Affairs
VeriSign Communications Services Div.
21355 Ridgetop Circle
Dulles VA 20166-6503
tel: +1 703.948.4305
mailto:trutkowski@verisign.com

Raj Puri
Vice President, NetDiscovery Service
487 East Middlefield Road
Mountain View CA 94043-4047
tel: +1 650.996.2927
mailto:rpuri@verisign.com

Michael Aisenberg
Director, Government Relations
1666 K Street, N.W., Suite 410
Washington DC 20006-1227
Tel: +1 202.973.6611
mailto:maisenberg@verisign.com

Brian Cute
Director, Government Relations
1666 K Street, N.W., Suite 410
Washington DC 20006-1227
tel: +1 202.973.6615
mailto:bcute@verisign.com

Filed: 21 December 2004

EXECUTIVE SUMMARY

Nearly every service provider and vendor or their representative organizations filing comments in this proceeding recognized the importance of providing real-time forensic evidence support capabilities for law enforcement that constitutes the purpose of CALEA. Many noted that the provision of these lawful interception capabilities also enhances the privacy of customers by implementing a structured process with checks and balances that are also part of CALEA.

This result should not be surprising. IP-Enabled Service providers have long implemented similar capabilities to detect, manage and protect their own network infrastructures from fraud and operational harm engendered by purposeful attacks or unintentional misconfiguration. Many species of cybercrime exists today on a significant scale and cooperation with law enforcement is essential. As a result, lawful interception capability requirements for IP-based Next Generation Networks have been established worldwide through national legislation and intergovernmental agreements. Product and service vendors must meet these global capability requirements – who have cooperated with law enforcement agencies to produce the necessary standards – and implemented the resulting specifications.

Although there is substantial disagreement among the commenting parties on the application of CALEA to these new networks, it seems plain by any reasonable reading of CALEA provisions and legislative history that Congress intended the Commission to evolve the law enforcement support capability requirements concurrently with network technology advances. The open characteristics of IP-Enabled Next Generation Networks today, coupled with increasing nomadicity and dispersion of criminals, necessitates ubiquitous national coverage with consistent handover interfaces to the thousands of law enforcement agencies nationwide who may require the forensic support.

There is only one significant substantive issue in this proceeding – who bears the cost burden for timely implementation, maintenance, and continuing evolution of the CALEA capabilities. As many commentors noted, it is a "scale issue." When spread across the entire national infrastructure, the cost per user is minimal. Moreover, the availability of Trusted Third Parties – as highlighted in the Commission's NRPM – will allow services providers to minimize resulting compliance costs. Performing CALEA support activities as the agent of a carrier/provider is technically and administratively similar to myriad infrastructure support capabilities routinely provided as part of commercial operations today. As a leader in providing CALEA and many other trusted third party services for the industry, VeriSign has already implemented and made commercially available CALEA requirements for various VoIP service providers and stands ready to implement CALEA requirements on a cost-effective basis for other IP-based Next Generation Networks.

In addition to proceeding with establishing and enforcing the requirements, the Commission can usefully reduce costs further by insisting on effective modularization and versioning of requirements and global standards, coupled with cost-sharing mechanisms to alleviate possible burdens on providers in underserved areas.

The comments and extrinsic facts support the Commission's CALEA-based requirements framework for law enforcement support capabilities for Next Generation Network/IP-Enabled broadband access and managed/mediated VoIP services

1. Nearly every provider and vendor or their representative organizations filing in this proceeding recognized in their comments the importance of providing real-time forensic evidence support capabilities for law enforcement that constitutes the purpose of CALEA.[1]

2. An overwhelming array of public factual material, coupled with the similar capability requirements being established and implemented worldwide, including international agreements, plainly refutes the comments by those parties who argue that Commission action in this proceeding is not timely or needed.[2] The open characteristics of IP-Enabled Next Generation Networks today, coupled with increasing nomadicity of users and dispersion of cybercriminals, necessitates ubiquitous national coverage with consistent handover interfaces to the thousands of law enforcement agencies nationwide who may require the forensic support pursuant to judicial order.

---

[1] *See, e.g., Comments*, BellSouth at 3-4; *Comments of CTIA – Tne Wireless Association™* at 2; *Comments of Global Crossing North America, Inc*. at 1; *Comments of Level 3 Communications, LLC* at 1; *Comments of Motorola, Inc*. at 1-2; *Comments of the National Cable & Telecommunications Association* at 1-5; *Comments of Nextel Communications, Inc.* at 1; *National Telecommunications Cooperative Association Comments in Response to the Notice of Proposed Rulemaking and the Initial Regulatory Flexibility Analysis* at 1; *Comments of the Coalition for Reasonable Rural Broadband CALEA Compliance* at 1-2; *Comments of the Rural Telecommunications Providers* at 1; *Comments of SBC Communications* (SBC Comments) at 3; *Comments of the Satellite Industry Association* at 1-2; *Comments of the Telecommunications Industry Association* at 1; *Comments of T-Mobile USA, Inc. on Notice of Proposed Rulemaking* at 1; *Comments of the United States Telecom Association* at 1-2; *Comments of Verizon on Commission's Notice of Proposed Rulemaking and Declaratory Ruling* (Verizon Comments) at 1, in ET Docket No. 04-295.

[2] *See, e.g.*, CALEA Implementation, Federal Bureau of Investigation, *Packet Surveillance Fundamental Needs Document (PSFND) for Telecommunications Carriers, Equipment Manufacturers, and Providers of Telecommunications Support Services*, Issue 1.0, 31 Oct 2001; CALEA Implementation, Federal Bureau of Investigation, *Electronic Surveillance Needs for Carrier-Grade Voice over Packet (CGVoP) Service*, Issue 1, 29 Jan 2003; CALEA Implementation Unit, Federal Bureau of Investigation, *Electronic Surveillance Needs for Public IP Network Access Service (PIPNAS)*, Issue 1, 30 Sep 2003; Telecommunications security; *Lawful Interception (LI); Technical Specification, Requirements of Law Enforcement Agencies*, ETSI TS 101 331 V1.1.1 (2001-08); *Convention on Cybercrime*, Budapest, 23.XI.2001. *Cf. Center for Democracy & Technology, Joint Comments of Industry and Public Interest* (CDT Comments) at 1-10 in ET Docket No. 04-295.

3. Even those arguing that CALEA does not apply to broadband access or managed/mediated VoIP services based on their reading of the 1994 Act, underscore the critical importance of the support - in many cases describing support already provided in the ordinary course of operation of their business. Broadband access and managed/mediated VoIP service providers today routinely build many of these same capabilities into their network infrastructures. The capabilities are essential to detect, manage and protect their own facilities from fraud and operational harm engendered by purposeful attacks or unintentional misconfigurations.

4. Many species of cybercrime exist today on a significant scale and cooperation with law enforcement is essential to protect provider networks and their customers. As a result, lawful interception capability requirements for IP-Enabled Next Generation Networks have been established worldwide through national legislation and intergovernmental agreements.[3]

5. Product and service vendors must meet these global capability requirements, and have cooperated with law enforcement agencies to produce the necessary standards – and implemented the resulting specifications. Indeed, several entire industry segments enthusiastically and expeditiously developed and implemented the necessary standards to provide the capabilities sought by law enforcement. This included cable-based telecommunication providers, carrier-grade Internet equipment vendors, and advanced wireless equipment vendors.

6. It seems plain by any reasonable reading of CALEA provisions and legislative history that Congress intended the Commission to evolve the law enforcement support capability requirements concurrently with fundamental network technology advances.

---

[3] *See, e.g., Cybercrime Convention, supra*; European Union, *Council Resolution of 17 January 1995 on the lawful interception of telecommunications*, Official Journal C 329 , 04/11/1996 P. 0001 – 0006; Canada, Department of Justice, *Lawful Access FAQ*, http://canada.justice.gc.ca/en/cons/la_al/summary/faq.html; Netherlands, Ministry of Economic Affairs (EZ), Directorate-General for Telecommunications and Post, CO, LM, EE, EL & SJ, WAI/GT/FuncSpecs, *Functional specifications lawful interception of Internet traffic in The Netherlands*, V1.0.1, June 2000; United Kingdom, Home Office, *The Regulation of Investigatory Powers Act (RIPA)*, http://www.homeoffice.gov.uk/crimpol/crimreduc/regulation/; Australian Communications Authority, *Internet Service Providers Interception Obligations*, http://internet.aca.gov.au/acainterwr/consumer_info/fact_sheets/industry_fact_sheets/fsi12.pdf; Germany, Regulatory Authority for Telecommunications and Post, *Technical Directive: Requirements for implementing statutory telecommunications interception measures (TR TKÜ)*, Ver. 4.0, Apr 2003; Republic of South Africa, No. 70 of 2002: *Regulation of Interception of Communications and Provision of Communication-related information Act, 2002*, Government Gazette, Vol. 451 Cape Town 22 January 2003 No. 24286.

The argument advanced by some parties is that the narrow "information services" exception in the 1994 Act denies law enforcement broadband access and VoIP CALEA capabilities because the exception equates to the "Internet," and the use of an Internet Protocol by the emerging IP-Enabled Next Generation Network infrastructure excludes the application of CALEA requirements.[4] However, this argument flies in the face of a massive array of regulatory and standards developments domestically and internationally all directed at establishing broad, comprehensive regulatory and standards frameworks for dealing with these services as part of the global public telecommunications infrastructure.[5] Congress plainly did not intend CALEA only to apply to telecommunication technology as it existed in 1994, and that once Internet Protocols based facilities started to be deployed as part of the public telecommunication infrastructure, CALEA requirements would cease to exist.

7. The Commission should also reject the "pseudo-technical" arguments that "packet" technology is fundamentally different or new, and poses fundamental challenges requiring new Congressional action and statutory provisions.[6] Ironically, digital packet technology goes back to the electrical telegraph with human operators providing manual switching. [7] Even contemporary computer-based packet-technology began being extensively used in public telecommunication networks in the 1970s, and today virtually all networks and network devices consist of packet-based computer implementations. What is "call data" versus "call content" in contemporary packet-based networks is well

[4] *See, e.g., CDT Comments* at 14-23, *Comments of the American Civil Liberties Union on the Notice of Proposed Rulemaking* (ACLU Comments) at 2-3; *Comments on Notice of Proposed Rulemaking of American Association of Community Colleges et al.* at 4-16; *Comments of the Electronic Frontier Foundation* at 8; *Comments*, BellSouth, at 5-11; Comments of Global Crossing North America, Inc., at 3-5; Comments Of Level 3 Communications, LLC at 9-11; *Comments of T-Mobile USA, Inc. on Notice of Proposed Rulemaking* at 3-8; *Comments of the United States Internet Service Provider Association* at 5-16.
[5] *See, e.g., Notice Of Proposed Rulemaking, In the Matter of IP-Enabled Services*, WC Docket No. 04-36, 10 Mar 2004; President's National Security Telecommunications Advisory Committee, Next Generation Networks Task Force; European Commission, *Commission Staff Working Document on The treatment of Voice over Internet Protocol (VoIP) under the EU Regulatory Framework*; Brussels, 14 Jun 2004; International Telecommunication Union, Telecommunication Standardization Sector, *Next Generation Networks (NGN) 2004 Project*, http://www.itu.int/ITU-T/studygroups/com13/ngn2004/index.html; OECD Working Party on Telecommunication and Information Service Policies, *Next Generation Network Development in OECD*, Doc. DSTI/ICCP/TISP(2004)4, 18 May 2004; Alliance for Telecommunications Industry Solutions, *Next Generation Network (NGN) Framework*, Issue 2.10, Oct 2004.
[6] *See, e.g., ACLU Comments* at 2-5.
[7] *See* Tom Standage, **The Victorian Internet**, 1998.

understood and clearly reflected in the many lawful interception standards and implementations that now exist – with ample safeguards.

8. Although a number of parties argued for the rejection of law enforcement's proposed framework for benchmarks, compliance deadlines, extensions, and CALEA enforcement, it seems unrealistic to expect the capabilities will be otherwise implemented to provide the necessary common capabilities and handover interface. The IP-Enabled Next Generation Network world is highly disaggregated and diverse. If the implementation of CALEA capabilities over the past decade has been problematic and difficult within a relatively stable and small number of regulated common carrier providers, a "blanket extension" approach for all "packet-mode" communications seems highly unlikely to be successful.

9. The mediated/managed VoIP distinction seemingly reflects industry practice, and appears to be largely supported by most commenters.[8] Indeed, from a notice standpoint, the distinction creates a useful contamination theory approach. If a communication is purely peer-to-peer, there is no obligation for anyone but the access provider because there is no additional signalling involved beyond that communicated directly between the communicating parties. However, if some entity provides some additional facilitating service as a public offering, that provider will be obligated to provide such call data that is mandated by law enforcement for every entity providing that service. The U.S. DOJ provides extensive criteria in this regard.[9] VeriSign agrees, however, with parties urging a clarification on what constitutes "reasonably available." This includes Cingular's suggestion that "CII held by another carrier or not accessible at an intercept access point is not "reasonably available," as well as CDT's suggestion that "only information that is "reasonably available" is information that the application provider already creates and/or obtains for its own business or technical purposes."[10]

10. Some commenting parties also underscored the importance of these Commission actions in enhancing customer privacy. This occurs in many ways –

[8] CDT, however, argues the distinction is "unclear" and "may lack…practical consistency." *CDT Comments* at 41.
[9] *See Comments of the United States Department of Justice* (USDOJ Comments) at 32-33.
[10] *Comments of Cingular Wireless LLC* (Cingular Comments) at 19; *CDT Comments* at 44.

principally by implementing a structured process with checks and balances – and is a basic objective of CALEA.

The principal issue in this proceeding revolves around the question of who bears the costs for the imposed capability requirements

11. Most of the comments in this proceeding were directed at one issue – who bears the cost for the capability requirements. Two cost dimensions are involved: initial capital equipment and continuing maintenance. The former consists of two components – typically rather low cost access devices, and rather high cost mediation systems that manage some significant number of access devices. The latter encompasses verification and compliance testing, security office requirements, and upgrades to the technical specifications.

12. As many commentors noted, costs are a "scale issue." When spread across the entire national infrastructure, the cost per user is minimal, and is highly unlikely to adversely affect either broadband or VoIP deployment.[11] The assertions by some parties that compliance is inherently costly is refuted by the facts.[12] Among individual broadband access and VoIP installations, utilization of a common service bureau can share the mediation capital equipment and continuing maintenance costs. Indeed, the costs are small enough that the service is attractive to operators of private networks who are motivated by considerations unrelated to CALEA, such as protecting their networks and customers from harm.

Almost every commenting party strongly supported the use of Trusted Third Party service bureaus to meet the capability requirements

13. Notwithstanding CDT's assertion that Trusted Third Party providers cannot estimate cost savings of alternative architectures, VeriSign does exactly this for its

[11] *Cf. AMA TechTel Communications, LLC Comments*
[12] *See Comments of Subsentio, Inc.*

prospective customers.[13] Performing this analysis is a fairly straightforward exercise of accounting for a handful of cost variables. The Commission should also reject on its face CDT's assertion that existing Trusted Third Party provision of CALEA support services to broadband access and VoIP providers can "offer absolutely no factual evidence" that the Commission should consider.[14] VeriSign's implementation of these capabilities for customers over the past two years is very relevant factual evidence that the Commission should consider.

14. Major carriers were quite positive in their comments. For example, "Cingular is generally supportive of the service bureau approach, as it provides carriers with competitive alternatives among different vendors and could help mitigate carriers' cost burdens."[15] "Verizon concurs with the Commission's conclusion that a 'Trusted Third Party' approach can be a useful method of helping some carriers comply with CALEA."[16] "SBC believes the Commission should allow, but not require, telecommunications carriers to use TTPs to meet their CALEA compliance obligations. TTPs could prove to be a more cost effective solution than having each carrier subject to CALEA take on all compliance responsibilities itself."[17]

15. On the issue of oversight of Trusted Third Parties, or the imposition of some kinds of additional regulatory requirements peculiar to the use of such Parties, Cingular observes that "generally, contractual arrangements and nondisclosure agreements would be adequate to address [the privacy and security of communications and that] such arrangements, combined with the possibility of an enforcement action being brought by LEAs under 18 U.S.C. § 2522, would adequately ensure a carrier's compliance with its obligations."[18] VeriSign concurs with Cingular's view here. Contractual agreements are preferred in dealing with potential security and privacy concerns.[19] Trusted Third Parties in their agency legal relationship must support whatever requirements or best practices are can be expected to meet whatever specifications are imposed on CALEA carriers. In addition, necessary most Trusted Third Parties compete in the marketplace on the basis of

[13] *See CDT Comments* at 51.
[14] *Id*. at 52.
[15] *Cingular Comments* at 20.
[16] *Verizon Comments* at 23.
[17] *SBC Comments* at 18.
[18] *Cingular Comments* at 20.
[19] *See USDOJ Comments* at 52.

security and privacy enhancements to provide a compelling value proposition to customers.

16. Although the ACLU finds the use of Trusted Third Parties "troubling" for privacy reasons – the reality is that the outsourcing of telecommunication and data processing functions has been a fundamental component of the business world since the inception of these technologies.[20] Performing CALEA support activities as the agent of a carrier/provider is technically and administratively similar to managing provider signalling infrastructure, billing records, controlling SPAM, mitigating fraud, providing network management, or performing any of a myriad of infrastructure support capabilities routinely a part of commercial operations today, and was contemplated in the Commission's earlier CALEA actions.[21] Indeed, the many additional legal requirements and liabilities surrounding the implementation of interceptions generally results in far more privacy protections than normal – whether it is additional authentication, legal review, or security support. The ACLU's assertion that Trusted Third Parties are somehow less secure or result in reduced protections is simply a hypothetical argument without basis or merit. It also ignores the significant security enhancement initiatives undertaken by Trusted Third Party providers.[22] VeriSign does, however, agree with the ACLU's comment that law enforcement run facilities should not be regarded as Trusted Third Party service bureaus.

17. The Electronic Frontier Foundation asserts that the use of Trusted Third Parties service bureau to provide a carrier's CALEA obligations would constitute "abdication of a traditional government function."[23] However, no explanation is

---

[20] See *ACLU Comments* at 9.

[21] The Commission has never placed any constraints on telecommunication carriers outsourcing operational or regulatory requirements to third parties. Indeed, in the context of outage reporting requirements, Third Party providers were explicitly treated by the Commission. *See Report and Order and Further Notice of Proposed Rulemaking*, in ET Docket No. 04-35, 19 Aug 2004. Indeed, outsourcing is the bedrock of the telecommunication industry, as even the largest providers frequently contract specialized operations and activities to third parties. Specifically with respect to CALEA obligations, the *Third Report and Order* and the adopted rules allow implicitly for Third Party outsourcing of the capability requirements, and have been explicitly accepted by the FBI CALEA Implementation Unit and the Commission as sufficient. *See Third Report and Order* in the Matter of Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, FCC 99-230, 31 Aug 1999.

[22] *See, e.g.,* OASIS *LegalXML Lawful Intercept (LI-XML) TC Charter,* Oct 2001;

[23] *EFF Comments* at 25.

provided as to how the implementation of CALEA requirements under the Commission's rules is a "traditional government function." The EFF goes further, stating:

> …VeriSign offers a legal intercept service to ISPs, which requires the providers to pipe all their data to VeriSign. Then VeriSign's employees then process the court order, analyze the data, extract information relevant to the court order, and send it to law enforcement.[24]

EFF offers no citation of any kind for its statement. VeriSign has no such offering, nor has it held out that it intends to provide such a service. Indeed, in the instant proceeding VeriSign stated in its comments that the EFF-described architecture is not advisable. EFF then uses this purportedly factual information, and references an ACLU paper on "conscripting businesses and individuals in the construction of a surveillance society" to paint a trusted third party treatment in the Commission's NPRM as "creating a surveillance-industrial complex…[where] private surveillance providers will profit from an increased amount of surveillance, and will have an incentive to lobby for more government surveillance powers and looser protections for users, further endangering privacy."[25]

18. VeriSign has long pioneered in developing and implementing security, authentication, and other trust technologies to mitigate against the very evils that EFF perceives as resulting from Trusted Third Parties. We submit that any objective analysis of Trusted Third Party use would result in a finding that the very privacy objectives that EFF seeks to promote (and which VeriSign support), are in fact enhanced with an independent service bureau.

Although the time to act is now, the Commission can take additional actions to further reduce the burdens and costs

19. The U.S. DOJ on behalf of law enforcement underscored in its comments the importance of timely compliance and an effective means of enforcement. CALEA implementation for broadband access or managed/mediated VoIP services is a critical public safety need that deserves due diligence by the Commission for many different reasons that include critical infrastructure protection and privacy enhancement, as well as mitigating crime and terrorism. The recent filing of one of the leading vendors of LI

[24] *Id*. at 26.
[25] *Id*. at 26-27.

equipment to implement these capabilities in over fifty countries underscores the reality that the solutions exist now and that "a cost effective solution can be created to meet the needs of the customer and we will continue to develop CALEA compliant solutions as technologies change and as the standards evolve."[26] Even small nations with less of a need for these capabilities and strong privacy values like The Netherlands, expeditiously took nearly five years ago the steps now being contemplated in this proceeding.[27]

20. In addition to proceeding with establishing and enforcing the proposed CALEA requirements, the Commission can usefully reduce costs further by insisting on effective modularization and versioning of requirements and global standards, coupled with cost-sharing mechanisms to alleviate possible burdens on providers in underserved areas. This subject was discussed extensively in VeriSign's comments in this proceeding, and the articulated solutions would diminish the cost concerns expressed by small and rural providers in this proceeding.[28]

The Commission should treat additional significant law enforcement support capabilities in a subsequent phase of this proceeding

21. Although few commentors in the proceeding treated three major ancillary topics – authenticated user/provider directory information, efficient request and handover of stored data, and transnational service bureau implementations – contemporary developments continue to underscore the critical importance of these matters, and the need for the Commission to treat them in a subsequent phase of this proceeding. The ability of law enforcement to quickly and effectively discover and access authenticated directory information is especially critical. If law enforcement cannot gain access to authenticated information concerning the service provider and user of communication identifiers such as E.164 numbers, IP-addresses, SIP addresses, all the CALEA support capabilities are almost worthless.

[26] *Comments of Verint Systems Inc*. at 9.
[27] *See* n. 3, *supra*.
[28] *See Comments of VeriSign, Inc*. at 23.

22. The requirement for the availability of and access to provider and user information of this nature has recently been introduced within the context of the NSTAC NGN Working Group and R&D Conference, as well as the International Telecommunication Union Standardization Sector's Next Generation Network Study Group.[29] VeriSign urges the Commission to treat in the instant proceeding, the critical CALEA need for a standards-based capability that allows 1) the discovery of basic authenticated provider and user information associated with broadband access and managed/mediated VoIP services, and 2) expeditious, secure access to that information.

[29] *See The Directory as critical intelligent infrastructure for NGN protection, NS/EP and other national needs*, NSTAC R&D Workshop, Monterey, 28-29 Oct 2004; *The NGN Directory Framework – Architecture and Protocols*, ITU-T SG 13 (NGN) Meeting, Doc. COM 13-D65-E, Geneva 7-17 Dec 2004.