

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

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

Reply Comments of VeriSign, Inc.

Further Notice of Proposed Rulemaking

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

Peter Wiederspan
Director, NetDiscovery Service
4501 Intelco Loop SE
Olympia, WA 98503
tel: +1 360.493.6220
mailto:pwiederspan@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 2005

EXECUTIVE SUMMARY

The relatively small number of commenting parties fall into four categories: 1) those rearguing the *First Order* and opposing its actions on broad jurisdictional grounds, 2) campus or rural access providers seeking temporary or permanent relief on jurisdictional and/or substantive bases; 3) VoIP providers seeking to limit the scope of related CALEA requirements, and 4) parties such as VeriSign that seek to provide needed forensic capabilities for law enforcement and critical infrastructure protection on reasonable and effective bases.

VeriSign suggests that this NPRM phase of the proceeding is not an appropriate venue for those parties continuing to argue fundamental issues of jurisdiction and authority that were decided in the *First Order*. On the remaining issues dealing with capability requirements for campus networks, “extranets,” networks serving rural and other high cost areas, and non-PSTN connected VoIP provisioning, VeriSign believes that a combination of service bureau implementations, coupled where necessary with Universal Service Fund (USF) support, can provide equitable and effective solutions to all the arguments raised to forestall CALEA capabilities. Similar to other public interest requirements, it is also critically important that these CALEA capabilities include the secure availability of authoritative subscriber identity information to law enforcement.

A. Broad jurisdictional challenges should be rejected

1. EPIC raises arguments proffered over the past decade that CALEA applies only “...to telecommunications carriers that use the public switched telephone network.”¹ EPIC even rejects the inclusion of any “packet-based communications,” which largely eliminates CALEA requirements for most of the communications infrastructure today. CDT, EFF, and Pulver are more focused in arguing that the Commission lacks the statutory authority or factual foundation to impose CALEA requirements on non-interconnected VoIP service providers.² Diverse universities operating campus networks also argue that their networks in whole or in part are excluded by CALEA’s private

¹ Electronic Privacy Information Center (“EPIC”) comments filed 14 Nov 2005 at 4.

² See Joint Comments of the Center for Democracy & Technology, Electronic Frontier Foundation, and Pulver.Com, filed 14 Nov 2005.

network exception and therefore the Commission lacks authority to impose CALEA requirements.³

2. As articulated in VeriSign's *Opposition* to the Stay requested by these same parties pending their judicial appeal, ample statutory bases exist both under CALEA as well as Title I of the Communications Act to support the Commission's actions both in the *First Order* and being considered in this Further NPRM.⁴ Today's IP-enabled public telecommunications infrastructure spans diverse kinds of physical and logical networks for which a bright public vs. private demarcation does not exist. Critical national infrastructure requirements such as those supporting law enforcement, national security, public safety, infrastructure protection, emergency preparedness, etc. should not be completely disabled by some broad assertion of "privateness" unless the network is physically and logically separate and independent from all infrastructure available to the public. Once interconnection and gateways exist, some reasonable, tailored requirements - that address the objectives sought - should be applied by the Commission. Such requirements for interconnected systems of networks have long been imposed by the Commission under the Communications Act, and CALEA additionally manifests equivalent authority under Sec. 102(8)(B)ii.

B. Trusted Third Party Service Bureau based CALEA implementations can meet the needs of all parties

3. Substantively, none of the parties commenting in the proceeding dispute the need to provide the required Internet access or "extended" VoIP network forensics for the purposes of assisting law enforcement or protecting critical infrastructure. (As used here, "extended" means third party assisted VoIP signalling such as SIP and H.323 based services that are not interconnected with the PSTN but equivalent to PSTN signalling services.) The various commenting university, library, VoIP, and small access providers

³ See, e.g., Comments of the University of California on Further Notice of Proposed Rulemaking; Comments of American Association of Collegiate Registrars and Admissions Officers, et al., (The "Higher Education Coalition"), filed 14 Nov 2005.

⁴ See VeriSign, Inc. Opposition Request for Stay Pending Issuance of Subsequent Orders and for Stay Pending Judicial Review Center for Democracy and Technology, et al., filed 2 Dec. 2005.

and their representatives assert vague potential difficulties and costs, but none dispute the need.⁵

4. DOJ, Verizon, BellSouth and VeriSign share the view that all providers of voice telephony services should be subject to similar CALEA network forensic support requirements, and focus on specific cases of relief as necessary.⁶ Today, many SIP-based VoIP signalling providers do not facilitate PSTN interconnection, and after the transition to a fully IP-enabled Next Generation Network architecture occurs, there will be no interconnection.⁷ It would be utterly inconsistent with CALEA for the Commission to establish a transition plan that envisions as an end goal, the complete elimination of telephony lawful interception support for law enforcement. This fundamental flaw in the scope of the *First Order* needs correction.

5. As Subsentio's analysis makes clear, the principal implementation costs reside in the mediation equipment, maintenance, and security office requirements – most of which are subject to very significant cost reductions through the use of Trusted Third Party service bureau.⁸ Subsentio asserts the large-scale shared implementation costs using a trusted third party service bureau are approximately “1 cent per subscriber per month or less.”⁹ VeriSign urges the Commission to consider this CALEA compliance approach to compliance for all broadband Internet access and signalling facilitated VoIP provisioning.

⁵ See Comments of the University of California on Further Notice of Proposed Rulemaking; Comments of American Association of Collegiate Registrars and Admissions officers, et al., (the “Higher Education Coalition”); Comments of the American Library Association and Association of Research Libraries; Comments of the Corporation For Education Network Initiatives in California, et al., In Response to Further Notice of Proposed Rulemaking; Comments of Skype Technologies, S.A.; Comments of the Telecommunications Industry Association; Initial Comments of Smitcoms, Inc.; Comments of the Information Technology Industry Council; American Cable Association, Comments; Comments of Earthlink, Inc.; Comments of the National Telecommunications Cooperative Association and the Organization for the Promotion and Advancement of Small Telecommunications Companies – all filed 14 November 2005.

⁶ See Comments of the United States Department of Justice; Comments of Verizon on the Commission's Further Notice of Proposed Rulemaking; Comments of Verizon on the Commission's Further Notice of Proposed Rulemaking – all filed on 14 November 2005.

⁷ See, e.g., SIP Center VoIP providers list, <http://www.sipcenter.com/sip.nsf/html/Service+Providers>; Voip-List.com <http://www.voip-list.com/>.

⁸ See Comments of Subsentio, Inc. filed 11 November 2005.

⁹ *Id.* at 6.

C. All CALEA capability requirements must include availability of authoritative subscriber identity information

6. Whatever decisions are reached by the Commission concerning the scope and details of the CALEA lawful intercept capability requirements for IP-enabled services providers, it is especially important that CALEA Sec. 103 requirements dealing with the availability of authoritative subscriber identity information by the service provider be fully implemented with a standardized interface comparable to that available in the traditional telephony environment. In the existing PSTN and other legacy public infrastructure environments, some substantial steps are generally taken to achieve a measure of identity authentication coupled with the maintenance of identification information in authoritative directories with protected interoperable access.

7. These steps are important not only for law enforcements, but also for public safety, consumer protection, infrastructure protection, fraud prevention, National Security Emergency Preparedness, and other important interests to be met. Comparable authoritative interoperable directory capabilities must be effected by the service provider or their agent pursuant to CALEA Sec. 103 and Title I for public IP-enabled services. A suitable comparable standardized technology for this purpose has been developed by industry, globally adopted, and implementation capabilities exist in the marketplace.¹⁰

¹⁰ See ITU-T, Rec. E.115-2005, Computerized Directory Assistance. See also, IRIS - The Internet Registry Information Service (IRIS) Core Protocol, IETF RFC 3981, January 2005; Cross Registry Internet Service Protocol (CRISP) Requirements, IETF RFC 3707, February 2004.