

HOUSE COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET
Hearing on “Law Enforcement Access to Communications Systems in a Digital Age”
September 8, 2004

Summary of Testimony of Stewart A. Baker
On behalf of the Telecommunications Industry Association

We all can agree that ensuring lawful law enforcement access to communications is an important goal. But if we've learned anything in the last twenty-five years of regulatory history, it's that we can't turn off our brains once we are told that a new regulation will serve an important social goal.

Preventing highway deaths is an important social goal, too, and there's no doubt that we'd have fewer fatal accidents if the speed limit on interstate highways was lowered to 30 miles an hour. We won't do that, though, because the costs of such a regulation simply are not worth the added benefit. Today, though, there's a real risk that the government will impose the wiretap equivalent of a 30 MPH speed limit on some of our most innovative and lucrative new industries.

The risk of stifling innovation was well recognized ten years ago when Congress drafted the Communications Assistance for Law Enforcement Act (CALEA). CALEA gave law enforcement a limited role in influencing the course of future technologies, and it specified limited enforcement rules to protect industry's ability to innovate without a permission slip from government.

But the Justice Department has asked the FCC to overturn key aspects of that carefully balanced statute. And in its proposed NPRM, the FCC seems ready to accept the Justice Department's invitation. The NPRM oversteps the Commission's regulatory authority in serious ways. First, the FCC proposes to write an entire new regulatory program to turn CALEA into a new FCC regulatory program, something that was not thought necessary when CALEA was enacted, or in the ten years since. Second, the FCC seems willing to set aside CALEA's insight that industry knows more than government about how to design new telecommunications equipment. Rather than continue to encourage the development of common industry standards for giving law enforcement access to call information, the Commission seems poised to restrict the role of industry standards in CALEA. This is a bad idea. Third, the Commission is considering a request to cut off the possibility of compensation for government-mandated network modifications – even going so far as to suggest that it may act under a statute that the FCC has not interpreted, enforced, or administered for thirty-five years. Finally, TIA is concerned that the FCC will not allow adequate timelines for CALEA implementation in newly covered industries.

None of these radical measures is justified. Despite the crisis atmosphere fostered by the government, the Justice Department and law enforcement have never once used the enforcement powers that CALEA gives them. The only logical conclusion is that there has never been a single case – not one, not anywhere in the country, and not at any time in the last decade – in which the Justice Department thought it could prove that a carrier had failed to meet its CALEA obligation and that important evidence was being lost as a result. Before throwing out CALEA as a failure and substituting a new FCC regulatory program that will slow innovation and saddle industry with heavy costs, we suggest that the Justice Department and law enforcement use the tools that Congress provided ten years ago.

**HOUSE COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET
Hearing on “Law Enforcement Access to Communications Systems in a Digital Age”
September 8, 2004**

**Testimony of Stewart A. Baker
On behalf of the Telecommunications Industry Association**

Good morning. My name is Stewart Baker. Thank you for inviting me to testify today on behalf of the Telecommunications Industry Association (TIA). I am grateful for the opportunity to speak to you about the current status of law enforcement’s ability to access new and ever-evolving communications systems, including broadband and Voice over Internet Protocol (VoIP) networks. TIA is a national trade association of 700 small, medium and large companies that provide communications and information technology products, materials, systems, distribution services, and professional services in the United States and around the world. In addition to representing its members on global policy matters, TIA is accredited by the American National Standards Institute, (ANSI), to develop American National Standards used by the industry. TIA also produces and co-owns SUPERCMM, the largest annual communications industry conference and exhibition.

Let me begin by stressing that all of us on this panel want the government to have the tools that it needs to fight crime and terrorism. As a former General Counsel of the National Security Agency, I recognize that it is crucial to give law enforcement those tools. In fact, several months ago, I testified before the 9/11 Commission on the need for more aggressive use of government authorities to gather anti-terror information, and I cautioned about the risks of putting an undue emphasis on privacy concerns when pursuing terrorists. TIA also believes strongly that law enforcement needs to have the ability to conduct lawful surveillance of communications and to have lawful access to communications systems.

So we all can agree that ensuring lawful law enforcement access to evidence is an important goal – as important as preventing highway deaths or ensuring clean air or workplace safety. But if we’ve learned anything in the last twenty-five years of regulatory history, it’s that we can’t turn off our brains once we are told that a new regulation will serve an important social goal. No matter how important the goals they serve, some regulations make sense and some don’t. Some go beyond statutory mandates. Some impose burdens that are nowhere near being cost-effective, stifling new industries and sending jobs overseas. This, unfortunately, is the kind of regulation that the Justice Department and the FBI support imposing today.

Of course law enforcement access is a good thing, at least when done within the law. But preventing highway deaths is also a good thing, and there’s no doubt that we’d have fewer fatal accidents if the speed limit on interstate highways was lowered to 30 miles an hour. We won’t do that, though, because the costs of such a regulation simply are not worth the added benefit. The same is true for wiretaps – except that today, there’s a real risk that we will impose the wiretap equivalent of a 30 MPH speed limit on some of our most innovative and lucrative new industries.

The risk of over-regulating and stifling innovation is a risk that was well recognized ten years ago when Congress drafted the Communications Assistance for Law Enforcement Act (CALEA). I was in government when much of this drafting was done. CALEA was the result of a compromise that gave law enforcement a very carefully limited role in influencing the course of future technologies. Congress rejected the idea that the federal government should design or even have a veto over the design of new technologies. Instead, it set forth a very limited performance standard for wiretap access that would apply to a limited portion of the telecommunications industry. The law left lots of room for innovation and initiative. Industry was free to decide how to meet the wiretap requirement – industry had the right to set its own standards, which would provide

a presumptively valid safe harbor for compliance, and individual companies that didn't like the standard remained free to try something else if they thought they had a better idea. Telecommunications technologies could be freely deployed without government interference, even if they did not have a perfect wiretap solution. Law enforcement could sue a carrier that deployed such technologies, but the carrier could defend itself by showing that full wiretap capability was not reasonably achievable in its system, or by showing that law enforcement could get the same information elsewhere.

TIA and its member companies rose to that challenge. TIA has led industry standards development efforts under CALEA, working jointly with the Alliance for Telecommunications Industry Solutions' Committee T1 to issue the leading CALEA compliance standard, J-STD-025, and the recent revision for packet-mode services, J-STD-025B. In fact, TIA member companies have gone well beyond what CALEA requires. For example, many companies that manufacture cable and Internet telephony hardware have already voluntarily built in intercept capabilities, despite uncertainty about whether CALEA applies to those services.

Despite this effort, disputes have arisen about what CALEA requires. Rather than continue to follow the dispute resolution processes established by Congress in CALEA, however, the Justice Department has asked the FCC to overturn key aspects of that carefully balanced statute. And in its proposed NPRM, the FCC seems ready to accept the Justice Department's invitation. The NPRM oversteps the Commission's regulatory authority in serious ways. First, the FCC proposes to write an entire new regulatory program to interpret and enforce CALEA, something that was not thought necessary when CALEA was enacted, or during the ten years thereafter. Second, the FCC seems willing to set aside CALEA's insight that industry knows more than government about how to design new telecommunications equipment. Rather than continue to encourage the development of

common industry standards for giving law enforcement access to call information, the Commission seems poised to restrict the role of industry standards in CALEA. Third, the Commission is considering regulation that would cut off all avenues by which carriers can receive compensation for government-mandated network modifications – even going so far as to suggest that it may cut off reimbursements under a statute that the FCC has not interpreted, enforced, or administered for thirty-five years. Finally, TIA is concerned that the FCC will not allow adequate timelines for CALEA implementation.

On the first point, the FCC proposes that it should have a role in enforcing manufacturers' and providers' CALEA compliance, even though the statute clearly places enforcement in the hands of lawsuits to be brought by the Justice Department. But the FCC, citing its general enforcement authority under the Communications Act, tentatively concludes that it should promulgate CALEA rules that can be enforced against all entities deemed subject to CALEA.

The FCC's proposal is an end-run around the enforcement limits established in CALEA. Congress constructed a regime that gave carefully circumscribed enforcement power to the federal courts, and the Communication Act's general grant of authority to the FCC does not allow it to ignore the enforcement regime Congress established. In particular, the FCC's approach to implementing new enforcement regulations ignores the statutory defenses available to providers in enforcement actions. For example, in the enforcement regime established in CALEA, a company cannot be sanctioned unless law enforcement has no alternative method of getting the information it seeks through the enforcement action. Equally important, by threatening to use fines and cease-and-desist orders against noncompliant companies, the FCC will force innovators to get permission from the FCC and the Justice Department before deploying any new technology that falls into the wide grey zone created by the FCC's vague proposed regulations. An inventor who must get a

government permission slip before trying out his invention is not likely to be first to market. While American innovators are still cooling their heels in Quantico, waiting to explain a new technology to the FBI Lab, their competitors in Singapore, China, Japan, and Europe will be manufacturing already. The U.S. market will end up a laggard, getting technologies after they've been sufficiently proven in the rest of the world to justify the engineering and lobbying costs needed to get an assurance of CALEA compliance.

At bottom, it is important that any enforcement framework allow for flexibility. Often, there is no simple answer to the question of how CALEA should be implemented. Instead, decisions in this area require a sophisticated balancing of the costs and benefits of various approaches. The CALEA framework is driven by industry standards and consultation between industry and law enforcement. And this negotiation-based approach is well-suited to the complex environment of CALEA compliance. To replace this framework with a top-down regulatory enforcement approach within the FCC would merely add another burdensome layer of regulatory pressure to an already complex CALEA-compliance process.

Second, TIA is concerned that in implementing its proposed CALEA rules, the FCC calls into question the sufficiency of the existing standards process, which has served as the backbone for industry compliance with CALEA. Industry-led standards development efforts are critical to the cost-effective and successful implementation of CALEA. Congress recognized the integral role of the standards process when it enacted CALEA. For example, when Congress had to make a choice between innovation and law enforcement control over CALEA compliance, Congress chose innovation, with its eyes wide open. Congress knew that the FBI wanted authority to oversee and even dictate the technical details of equipment manufacturers' CALEA-compliant solutions. But Congress rejected that approach, and instead enacted CALEA with a provision that prohibited law

enforcement from requiring “any specific design of equipment, facilities, services, features, or system configurations.” (47 U.S.C. § 1002(b)(1).)

At the same time, in Section 107(a) of CALEA, Congress explicitly noted the special role it gave to industry in creating standards to meet CALEA obligations. Section 107(a) “establishes a mechanism for implementation of the [CALEA] capability requirements that defers, in the first instance, to industry standards organizations.” (H.R. Rep. No. 103-827, 1994 U.S.C.C.A.N. 3489, 3506 (1994).) But in order for this standards process to work effectively to address law enforcement’s needs, industry needs to have the support of regulators. And right now, that support appears to be lacking. The FCC in its CALEA NPRM questions whether existing standards are deficient and whether it should only recognize standards produced by certain organizations.

Further, law enforcement has been uncomfortable with the fact that CALEA gives the lead standards role to industry. Since CALEA was enacted, law enforcement has wanted to guide, if not dictate, the detailed CALEA solutions that industry may implement. While this has created considerable tension between law enforcement agencies and industry throughout the standards process, there is no evidence to suggest that industry standards participants have acted in anything other than good faith.

In fact, TIA, its member companies, and other participants in TIA’s standards activities have worked diligently – and cooperatively with law enforcement – for nearly a decade to adopt and improve CALEA standards and to ensure that law enforcement has access to appropriate, lawfully authorized electronic surveillance capabilities consistent with CALEA’s statutory requirements. TIA’s efforts led to the development of the J-STD-025 series of CALEA compliance standards, created at the expense of thousands of hours of industry experts’ time and months of meetings.

Instead of scuttling the standards process altogether, law enforcement should be required to identify with specificity what aspects of what standards it is challenging, and the particular ways in which it deems the standards to be deficient. Industry should be given the opportunity to respond to law enforcement's concerns. Industry has demonstrated its responsiveness and diligence in developing standards in the past, and there is no reason to doubt that this level of cooperation will continue.

A leading role for industry in CALEA standards-setting is essential to further Congress's goal "to avoid impeding the development of new communications services and technologies." (H.R. Rep. No. 103-827, 1994 U.S.C.C.A.N. 3489, 3493 (1994).) Industry is by far best situated to design CALEA compliance standards in a complex, rapidly changing technology environment. An industry-led standards process permits U.S. companies to press forward with technological innovation, which is one of the key drivers of the U.S. economy in recent decades. At the same time, an industry-led standards process affords industry appropriate lawfully authorized electronic surveillance capabilities for evolving communications technologies.

The FCC also has suggested that perhaps CALEA standards should be set only by ANSI-accredited bodies. That is not what CALEA requires, and for good reason. TIA is an ANSI-accredited body, and it has written CALEA standards, so you might expect us to be comfortable with such a proposed limitation. But we are not. ANSI procedures call for consensus standard-making, and, in some instances, law enforcement has tried to use this requirement to defeat standards that all of industry has supported – by asking hundreds of sheriffs and local police to join the standards process at the last minute, for example, for the purpose of voting against the industry standard. In addition, an ANSI-accreditation requirement would encourage harsh tactics, such as

the FBI's (now abandoned) effort to revoke TIA's accreditation after TIA adopted a standard that the FBI did not accept.

Third, TIA is concerned that manufacturers and service providers will be required to undertake expensive and burdensome network modifications in order to comply with CALEA under the FCC's proposed rules. Because the beneficiary of these changes are law enforcement agencies in the first instance and the general public in the last, one would expect that the cost of the changes would be carried largely by those parties. But the FCC's proposed rule puts the burden on industry, and it seems determined to make sure that there is no possibility of relief from the costs of CALEA. Instead, the FCC should reaffirm its previous conclusion that service providers may recover a reasonable share of CALEA costs that intercept law allows them to charge when carrying out a wiretap order. The principal mechanism for recovering those costs, Title III of the Omnibus Safe Streets and Crime Control Act of 1968, is far from the FCC's jurisdiction, and there is no need for the FCC to reach out now to determine that CALEA costs cannot be recovered under that statute.

Finally, TIA urges a reasonable timeline for requiring compliance with whatever rules the FCC eventually promulgates. Regulators and law enforcement must understand that industry needs a reasonable compliance deadline that creates enough space for equipment manufacturers, like the TIA members, to design and develop CALEA solutions well in advance of their actual deployment in the market.

In conclusion, I stress that, despite the crisis atmosphere fostered by the government, the Justice Department and law enforcement have never once used the enforcement powers that CALEA gives them. The only logical conclusion is that there has never been a single case – not one, not anywhere in the country, and not at any time in the last decade – in which the Justice Department thought it could prove that a carrier had failed to meet its CALEA obligation and that

important evidence was being lost. Before throwing out CALEA as a failure and substituting a new FCC regulatory program that will slow innovation and saddle industry with heavy costs, we suggest that the government try using the tools that Congress provided ten years ago.