

Computer Professionals for Social Responsibility
Susan Evoy, sevoy@cpsr.org, <http://www.cpsr.org/>
"Wiretapping The Internet: Is VoIP Different?"

Computer Professionals for Social Responsibility Comments on extension of CALEA to VoIP

This one-pager describes general considerations that illuminate current requests by law enforcement to extend CALEA's wiretapping requirements for telephone equipment to Voice over IP (VoIP). This paper does not discuss the value or appropriateness of CALEA. It asks only how the provisions for adapting telephone equipment for wiretapping can translate into the Internet realm.

Attempts to regulate VoIP are complicated by the vagueness of that term. No one speaks of "graphics over IP" because it is obvious that graphics exist in numerous formats and can be sent via email, downloaded as part of a Web page, transferred as independent files, or provided in other ways. Furthermore, graphics can be permanently stored or generated on the fly. The same rich variety of experience applies to voice transmission. Let us look at some results that emerge from the nature of Internet communications.

CALEA's provisions related to support for wiretapping were designed with physical equipment in mind. There are a limited number of physical telephone switches made by a limited set of manufacturers. While the cost of adapting them for wiretapping is significant (Congress allocated 500 million dollars in CALEA to pay the manufacturers for their effort, and the manufacturers complained that this was much too little) it can still be treated as a cost to factor into the overall cost of the equipment. CALEA assumes that the user enters the network at an identifiable point through a telephone provider's switch, that an identifiable entity (the telephone provider) has control over that switch, and that law enforcement can hold the telephone provider responsible for monitoring traffic.

VoIP demonstrates the typical problems of translating legal models for physical equipment to a software realm. Where does the transition to VoIP take place? It is in a software module, perhaps developed in open-source fashion and downloaded free by an end-user. The capture and translation of voice into IP packets can take place during an instant messaging session or as part of a larger application such as collaborative whiteboarding. By the time a switch is reached (if not before) VoIP is indistinguishable from other Internet traffic.

In short, there is an enormous range of developers and software components for VoIP; new ones are added all the time. The flexibility and low barriers to entry represent some of VoIP's most attractive and valuable traits. Requirements to allow wiretapping are both onerous and ultimately perhaps unenforceable.

One could imagine, for instance, that the government required everyone providing VoIP (stand-alone or as part of a larger application) to share the specifications for its protocols with the government. Law enforcement could then decode traffic at the Internet provider. But given the variety of protocols and the volume of traffic, such a regulation would place serious burdens on software developers, Internet providers, end-users, and law enforcement alike. Finally, a VoIP phone device in the United States could route its communications through an IP address outside of the U.S. and therefore outside of U.S. law enforcement jurisdiction.

The physical architecture of standard phone service, with clear entry and exit points, also impose inherent limits on monitoring; it can be restricted to the particular individuals permitted by court order. No such natural limits exist in VoIP software, so instrumenting it to allow monitoring would open the door to abuse both by law enforcement officials and malicious individuals with access to the equipment where conversion from voice to IP occurs.

Defining and fixing the endpoints to an Internet telephone conversation would require invasive hooks in Internet software that would expose to illegal search and seizure everyone who shares the IP network with the party that law enforcement has the authority to monitor. Collecting Pen Register or addressing data, in particular, would require proactive logging, forensics and filtering of all live data of everyone who shares the network with the suspect in question, subjecting others not targeted by law enforcement to illegal search and seizure.

Congress, in enacting CALEA, recognized that Internet traffic was an entirely different sort of animal and exempted that traffic from CALEA. The FCC has also tread carefully in the regulation of VoIP. It recognized the multiplicity of implementations by initially and tentatively applying long-distance telephone charges only to VoIP sessions that passed through a traditional central office switch on at least one end. Both Congress and the FCC held back from trying to nail the gellatin of pure Internet traffic to the wall.

In conclusion, it is likely that any extension of CALEA's wiretapping requirements to VoIP software will hamper its adoption among the general population but not prevent its use by criminals and terrorists, who can hide it (or find substitutes for it) in other forms of traffic.