Security, Wiretapping, and the Internet

In a move that is dangerous to network security, the US Federal Bureau of Investigation is seeking to extend the Communications for Law Enforcement Act to voice over IP. Such an extension poses national security risks.

Susan Landau
Sun Microsystems

Wiretaps have been used since the invention of the telegraph and have been a legal element of the US law enforcement arsenal for more than a quarter century. In keeping with law enforcement's efforts to keep laws current with changing technologies, in 1994 the US Congress passed the Communications Assistance for Law Enforcement Act (CALEA). The law proved to be controversial because it mandated that digitally switched telephone networks must be built wiretap enabled, with the US Department of Justice in charge of determining the appropriate technology standards.

The law provided a specific exclusion for "information services." Despite that explicit exemption, in response to a request from the US Federal Bureau of Investigation (FBI), in August 2005, the Federal Communications Commission (FCC) ruled that broadband voice over IP (VoIP) must comply with CALEA. Civil-liberties groups and the industry immediately objected, fearing the ruling's impact on privacy and innovation. There is another community that should be very concerned. Applying CALEA to VoIP requires embedding surveillance technology deeply into the protocol stack. The FCC ruling undermines network security and, because the Internet and private networks using Internet protocols support critical as well as noncritical infrastructure, national security as well. The FCC ruling is a step backward in securing the Internet, a national—and international—priority.

CALEA's history

In 1992, the FBI was struggling. What had been a boon for telephony—the split-up of AT&T (Ma Bell), which previously had a monopoly of the US market—was a serious problem for the bureau. Instead of implementing wiretaps by working with a single service provider and phone company, the FBI found itself facing a plethora of suppliers of services and telephones. Even worse from the FBI's perspective were the new telecommunications technologies: cell phones, call forwarding, call waiting, and speed dialing. That same year, the FBI put forth the Digital Telephony proposal, which would have required wiretapping standards to be included as part of the design of digital-switching telephone equipment.

The FBI claimed that the advanced calling features impeded court-authorized wiretaps. However, *The Washington Post* investigated and discovered that, "FBI officials said that they have not yet fumbled a criminal probe due to the inability to tap a phone."[1] At this news, Computer Professionals for Social Responsibility, a public-interest group, initiated Freedom of Information Act litigation; in response, the FBI released a four-page list of impeded cases in which, citing "national security," all information was blacked out.[2]

Digital Telephony proposal

The FBI's Digital Telephony proposal represented a sharp change in the government's approach to wiretapping. Instead of letting service providers determine how to configure their systems to accommodate wiretaps, the proposal put government in the middle of telephone-equipment design. In fact, this bill placed the US Attorney General, a position not generally known for technical expertise, into the process of standards design of

equipment used by the general public. Industry and civil-liberties groups opposed the FBI proposal, and no one in Congress would sponsor it.

In 1994, the FBI reintroduced the bill, and this time, events played out differently. Over the course of the Congressional session, the bill's scope changed, narrowing down to common carriers (rather than all electronic communication service providers), adding some protections for transactional information—the first time such information was afforded protection in wiretapping law—and eliminating a clause requiring telephone companies to decrypt encrypted conversations, regardless of whether they had an encryption key. There was also a sweetener for the telecommunications companies: a US$500 million authorization to help carriers update their networks to comply with the law's requirements. Although other civil-liberties groups had continued to oppose the bill, the Electronic Frontier Foundation's support of the final version—now renamed CALEA—helped persuade the telephone companies to support it. This time, the bill passed. Though the law governed just the US, its impact was far broader. The FBI pressed other nations to adopt similar laws. In any case, because the law applied to the US telecom market, much of the rest of the world was forced to adopt the standards that CALEA dictated.

Implementing CALEA

The law ran into trouble almost immediately. The telephone companies believed that negotiations on the bill had left them in a position in which standards would be determined through consultation with the FBI. After passage however, the FBI took the stance that the law allowed it to set requirements without consultation.

The FCC, which has jurisdiction over telecommunications regulations, and the courts have generally upheld the FBI's interpretation—even in cases in which CALEA excluded the FBI's proposed standards.[3] Although CALEA required telephone companies to meet the government's standards by 1998, disagreements between telecommunications companies and the FBI on appropriate standards meant the deadline could not be met. Congress was unhappy with the delay, and several Congressmen, including Senator Patrick Leahy (D-Vermont) and Representative Bob Barr (R-Georgia), pointed the finger at the FBI.

These disputes—and delays—concerned CALEA's application to telephony. CALEA's language specifically exempted information services: "The term 'telecommunications carriers'—(A) means ... a common carrier for hire; and (B) includes (i) ... commercial mobile service; or (ii) ... service that is a replacement for a substantial portion of local telephone exchange service ...; but (C) does not include ... information services."[3] Nonetheless, in late 2003, the FBI served notice to the FCC that VoIP providers would be subject to CALEA.

As was the case in 1992 with the Digital Telephony proposal, the FBI did not provide any examples of problems found in conducting law enforcement wiretaps on VoIP calls. In March 2004, the FBI, the US Department of Justice, and the US Drug Enforcement Agency submitted a joint petition to the FCC requesting that it rule on CALEA's applicability to VoIP. Over the next year, computer companies joined the anti-CALEA coalition of civil-liberties groups and telecommunications providers that formed in the 1990s. None objected to the idea of wiretapping voice calls—indeed, many companies were involved in determining appropriate ways to enable the tapping of VoIP calls—but all objected to the idea that the government should be involved in setting standards for interception on the packet-switched Internet. In August 2005, the FCC announced that broadband providers of VoIP must comply with CALEA.[4] CALEA, which mandates government role in standards design, is an oddity in US wiretap law, which we will briefly examine.

US wiretap laws

Wiretaps have had a long and complex history in US jurisprudence. Their first use was in the mid 19th century, in response to the invention of the telegraph. Shortly afterward, they appeared in war: Confederate General Jeb Stuart traveled with his own wiretapper to tap Union army lines.[5] Wiretaps came into their own during Prohibition, the period between 1920 and 1933 in which the manufacture and sale of alcohol was illegal. Federal law-enforcement agents discovered the value of wiretaps in both investigating and prosecuting bootlegging cases. The Olmstead case set the stage for the next 40 years of US wiretap law.[6]

A form of search

In the 1920s, Roy Olmstead had a major bootlegging operation in Seattle. Federal agents wiretapped Olmstead and his co-conspirators, placing taps in the basement of his office building and on telephone poles outside private houses. Olmstead's lawyers argued their case on the basis of the Fourth Amendment to the US Constitution:

> The right of the people to be secure in their persons, house, papers and effects against unreasonable searches and seizures shall not be violated, and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[6]

The US Supreme Court held that wiretaps were not a form of search, and thus didn't require search warrants.

But the most well-known opinion in the Olmstead case isn't that of the majority, but of Justice Louis Brandeis's dissent. He said that wiretaps were a special type of search:

The Court's rulings of the 1930s did not end law enforcement wiretapping; instead, tapping went underground figuratively as well as literally.

> The evil incident to invasion of privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may know or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wiretapping.
>
> —Olmstead v. United States[6]

A decade later, citing the 1934 US Federal Communications Act, which prohibited the "interception and divulgence" of wired communications, the US Supreme Court overturned the Olmstead decision in the Nardone cases.[7] In a series of cases over the next 30 years, the Supreme Court also slowly narrowed the circumstances under which law enforcement could perform electronic bugging without a warrant, until 1967, in *Charles Katz v. United States* when the Court concluded that an electronic bug in even so public a place as a phone booth was indeed a search and therefore should be protected under the Fourth Amendment.[8]

The Court's rulings of the 1930s did not end law enforcement wiretapping; instead, tapping went underground figuratively as well as literally. After the Nardone rulings, law enforcement didn't publicly divulge wiretapped information (or, it did, but not the fact that the information came from wiretaps). This legal never-never land led to abuses by FBI director J. Edgar Hoover's agents, including the wiretapping (and bugging) of political dissidents, Congressional staffers, and US Supreme Court Justices.[9–11] The FBI's extensive records on political figures was well known, and this information, some of which was salacious, ensured that Congress conducted little oversight of the FBI. When, in reaction to the *Katz* decision, Congress decided to pass a wiretapping law, the national legislature was quite concerned about preventing Hoover-era abuses.

Changing views

The complications of investigating organized crime—including victims' reluctance to testify, so-called victimless crimes (such as prostitution), and the corruption of local law enforcement—make electronic surveillance a particularly valuable tool. In 1967, a presidential commission investigating organized crime concluded, "legislation should be enacted granting carefully circumscribed authority for electronic surveillance to law enforcement officers ...."[12] In response, US President Lyndon Johnson signed the Omnibus Crime Control and Safe Streets Act of 1968, of which Title III legalized law enforcement wiretaps in criminal investigations. Because of wiretaps' invasive nature, the act listed only 26 crimes that could warrant wiretap investigations, including murder, kidnapping, extortion, gambling, counterfeiting, and the sale of marijuana. The US Judiciary Committee's report explained that "each offense was chosen because it was intrinsically serious or because it is characteristic of the operations of organized crime."[13]

Congress decided that stringent oversight of wiretapping should require a federal district court judge to review each federal wiretap warrant application. Although President Johnson had used wiretaps on civil-rights leader Martin Luther King Jr. during the 1964 Democratic Party convention and on US Vice President Hubert Humphrey in 1968, publicly, the president was ambivalent about wiretaps. Even as he described the Title III provisions for wiretapping as undesirable,[14] he signed the wiretapping provisions into law.

Title III

For criminal investigations (the only kind Title III addresses), wiretap warrants are more difficult to obtain than normal search warrants. The judge must determine that there's probable cause to believe

- an individual is committing, has committed, or is about to commit an indictable offense;
- communications about the offense will be obtained through the interception;
- normal investigative procedures have been tried and either have failed, appear unlikely to succeed, or are too dangerous; and
- the facilities subject to surveillance are being used or will be used in the commission of the crime.[15]

Title III covers procedures for obtaining wiretaps for law enforcement investigations. In 1972, in a court case involving "domestic national security issues," the US Supreme Court ordered an end to warrantless wiretapping, even for national security purposes.[16] "Domestic

national security" cases had fueled a large number of inappropriate investigations of Americans, including

- the US Central Intelligence Agency opening and photographing nearly a quarter of a million first-class letters without search warrants between 1953 and 1973;
- 300,000 individuals indexed on CIA computers and CIA files on 7,200 individuals;
- the US National Security Agency obtaining copies of millions of private telegrams sent to and from the US from 1947 to 1975 without search warrants through an arrangement with three US telegraph companies; and
- US Army Intelligence keeping files on 100,000 Americans.[10]

Because of the public outcry over the discovery of numerous Nixon administration "national security" wiretaps that had been conducted for political purposes,[10] it took until 1978 for Congress to craft the Foreign Intelligence Surveillance Act (FISA), which authorizes procedures for national security wiretapping. Congress considered it extremely important that safeguards be in place to prevent such illegal surveillance in the future.

Foreign Intelligence Surveillance Act

In contrast to Title III's requirements that a judge determine whether there's probable cause to believe that an individual is involved in committing an indictable offense, in FISA cases, the judge, a member of an FISA court, must determine whether there's probable cause that the target is a foreign power or agent of a foreign power. The purpose of the surveillance is to obtain intelligence information. The law provides that "[N]o United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States."[17]

The requirements for foreign intelligence wiretaps are less stringent than those for law enforcement. *United States v. United States District Court* held that domestic national security wiretapping must be conducted under a search warrant, and the US Supreme Court stated that, "Different standards [for gathering intelligence] may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."[16] National security investigations are more typically concerned with preventing future crimes rather than prosecuting previous ones, and the ability to present a case in court is often orthogonal to the real concerns of national security cases.

Title III and FISA form the basis for US wiretap law. State statutes also exist, with approximately half of all wiretaps for criminal investigations in the US performed using state wiretap warrants. The rules governing state wiretaps must be at least as restrictive as those governing Title III. There have been several updates and modifications to the federal wiretap statutes, including the Electronic Communications Privacy Act, CALEA, and the PATRIOT Act. In this article, my focus is solely on CALEA.

Communications in an age of terror

US wiretap laws were passed during an era in which the national threats were organized crime and civil unrest. In evaluating the efficacy of applying a CALEA-like law to the Internet, it's important to put today's threats into context and understand the new communications context.

Law enforcement and terrorism

The war on terror is the US's most pressing security concern, but it isn't actually a war on terror: it's a war against violent religious fundamentalists who use terror as a weapon. As a society, we have become accustomed to using "war" to refer to situations to which the word doesn't properly apply: "the war on drugs," "the war on poverty," even "the war on spam." In the case of violent fundamentalists—for Osama bin Laden and al Qaeda, this means violent Muslim fundamentalists—this is indeed a war.

Law enforcement concerns have governed domestic approaches to this war. In part, this is because we know how to catch so-called bad guys (or as Michael Scheuer says in *Imperial Hubris,* "[because if] bin Laden is a criminal whose activities are fueled by money—not a devout Muslim soldier fueled by faith—[...] Americans know how to beat well-heeled gangsters."[18]). The FBI's successful investigations of the Lockerbie plane crash over Scotland in 1988 and the first World Trade Center bombing in 1993 led the public and policymakers into believing the tools of law enforcement were appropriate for combating terrorism.[19] But the war against violent religious fundamentalists won't be won by law enforcement, which provides the wrong tools and the wrong incentives. For example, one of the most important functions of law enforcement is its deterrent value, but law enforcement isn't a deterrent to terrorists. Rather, violent fundamentalists often view a jail sentence as a form of martyrdom and an increased opportunity for recruiting.[20]

Even more basic to the distinction between law enforcement and national security investigations is that law enforcement and national security investigations have substantively different purposes. Law enforcement sees the solving of a crime as a success. Yet, when terrorism is concerned, prevention is the only real measure of success. Law enforcement seeks a level of proof that will convict a criminal in a court of law, which is inappropriate in a war

against terrorists. The type of intelligence work needed for national security investigations seeks different outcomes than those of criminal investigations, which are measured by arrests made and convictions obtained.

Applying CALEA to VoIP is a mistake: the insecurities that will result are likely to extend well past VoIP to other aspects of the Internet.

The events of September 11th, 2001 make it dreadfully clear that the law enforcement focus is inadequate for this war. Scheuer states it bluntly: "Bin Laden is leading and inspiring a worldwide anti-US insurgency; he is waging war while we fight him with counterterrorism policies dominated by law-enforcement tactics and procedures. It has not and will not work."[18] National security's emphasis on prevention is the critical aspect of this war.

Computer security and terrorism

What does all of this have to do with computer security? The Internet has proved a boon to many industries, and the last decade has seen a massive shift to it as the preferred form of conducting business. But the Internet is insecure. The network was originally designed to share resources, and neither security nor wiretapping were considerations in its initial design. Security is a serious concern for Internet users, which include many private industries that form part of critical infrastructure: energy companies and the electric-power grid, banking and finance, and health care. That's why applying CALEA to VoIP is a mistake: the insecurities that will result are likely to extend well past VoIP to other aspects of the Internet, and the end result will be greater insecurity.

Enter new technology: The Internet

Although it might look like a duck, walk like a duck, and quack like a duck, Internet telephony is not, in fact, a duck. It's a very different species from the circuit-switched telephony of Ma Bell.

Telephony vs. the Internet

At its bottom level—metal wires, optical fibers, microwave relays, and satellite channels—the public-switched telephone network (PSTN) and the Internet use the same resources, but the way they manage those resources is quite different. In circuit-switched telephony, a dedicated, end-to-end circuit is established for the call. Calls have time multiplexing, which means several calls may share a line. Either each call has a dedicated timeslot in every frame—called synchronized multiplexing—or there's an asynchronous version of the slots, in which each timeslot includes the call's identifier.

In the pre-computer telephone network, the route a call took was represented by the states of mechanical switches in the telephone offices through which the call passed. In a computerized network, the call is represented by table entries that show which incoming line is connected to which outgoing line. This is a commitment of resources that represents a significant cost for the network, a cost related to the traditional cost of a three-minute phone call. In digital terms, the resource commitment is optimized for communications that send thousands or millions of bits at a time.

The route that packets on the Internet take is determined not by entries in the network's tables, but by addresses carried in the packets. Packet progress through the network is affected by routing tables; these tables reflect the network's characteristics and not that of the individual communications. In theory—though less so in practice—each packet of a VoIP call can use a distinct path to reach its destination. This is the first problem that Internet wiretapping poses. On the Internet, routing control is distributed. It's impossible to determine a priori the routing of the packets the communication is broken into—this is determined by the routing tables, which change depending on the network traffic. Thus, unless the communication is tapped at the endpoints (at the user, or at the Internet service provider if the user always accesses the same provider), it's impossible to guarantee 100 percent access to all communication packets. From a privacy viewpoint and to address law enforcement's minimization requirement (that wiretapping be of a designated target—and not someone else using the line—and that the tapped call be related to the investigation), a further difficulty is posed by the fact that many other pieces of traffic travel along portions of the same path as the communication to be tapped. Thus, tapping anywhere but at the endpoints exposes other communications; this was one of the problems of the FBI's Carnivore (now renamed DCS-1000) system for tapping email. (Carnivore was an FBI Internet monitoring system designed to be installed at an ISP. The system "filtered" Internet communications and delivered target communications to a remote site, namely the law-enforcement agency. According to the FBI, only those communications that were subject to the wiretap order were forwarded to the FBI [www.fbi.gov/congress/congress00/kerr090600.htm]. The FBI has since shifted to using commercial software to conduct such investigations.)

Intelligence at the endpoints

The PSTN was architected throughout the system to have high quality for its most important application:

voice transmission. The endpoints—the phone receivers—are dumb. In considering the issue of architecting wiretaps into communications channels, a crucial difference between the PSTN and the Internet is that intelligence is at the endpoints for the Internet. The underlying network is deliberately simple, leaving the endpoints able to deploy complex systems.

The Internet design paradigm was chosen for flexibility:

> The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the endpoints of the communications system. Therefore, providing that questioned function as a feature of the communication system itself is not possible.[21]

The principle of letting the endpoints implement the function rather than having low-level function implementation be part of the underlying communication system is known as the "end-to-end" argument in system design. It is fundamental to Internet design. [22]

Intelligence at the endpoints enables versatility. Applications can be developed far beyond what the original designers of the communication system envisioned. Indeed, innovation on the Internet has flourished precisely because of applications. The flexibility afforded by the Internet design paradigm means there are few barriers to entry for a novel service, and the Internet boom of the late 1990s was greatly enabled by the low barrier to entry for new applications.

The layered approach to network design—application, transport, network, link, and physical—doesn't itself preclude wiretapping. It simply requires that wiretapping, an application, be handled in the application layer, or at the target's network connection. The whole issue of applying CALEA to VoIP exists to achieve 100 percent compliance with court-authorized wiretaps, but such compliance is impossible to guarantee at the application layer. Service providers do—and will—seek to comply with court-authorized wiretaps, but an end user who is determined to thwart a wiretap, perhaps through a complicated scheme of directing in which streams the traffic will run, will be able to do so. Without pushing wiretapping capabilities deeper into the protocol stack, it will be impossible to achieve 100 percent success for court-authorized VoIP wiretaps. And pushing wiretapping capabilities further into the network stack violates the end-to-end principle, which, although not sacrosanct, has proved quite valuable.

Building wiretapping into protocols

There is nothing inherent in the design of a communications network that rules out security or wiretapping, and indeed there are defense communications networks that provide both security and the capability of tapping. Had security or wiretapping been part of the Internet's core requirements, the functionality could have been built in from the beginning. There are secure government communication systems which, at (government) customer request, are capable of doing key recovery, thus enabling data recovery (wiretapping). The difficulty in designing these capabilities into the Internet occurs in attempting to securely implement wiretapping ex post facto into the current network architecture. The FBI petition to apply CALEA to VoIP is nothing less than a request to redesign Internet architecture.

In 2000, an Internet Engineering Task Force (IETF) Network Working Group studying the issue of designing wiretap requirements into Internet protocols observed that any protocol designed with built-in wiretapping capabilities is inherently less secure than the protocol would be without the wiretapping capability. Adding wiretapping requirements into network protocols makes protocols even more complex, and the added complexity is likely to lead to security flaws. Wiretapping is a security breach, and no one wants to see those breaches, deliberately architected or not. The IETF Network Working Group decided not to consider requirements for wiretapping as part of the IETF standards process.[23]

The IETF's warning is clear: Internet wiretapping can be used not only by those interested in protecting US interests, but also by those who oppose them. A technology designed to simplify Internet wiretapping by US intelligence presents a large target for foreign intelligence agencies. Breaking into this one service might give them broad access to Internet communications without the expense of building an extensive intercept network of their own.

In the spirit of modern computer-based industries, it seems likely that any intercept capability built into Internet facilities will be capable of the same remote management that's typical of the facilities themselves. This was the case, for example, with Carnivore. System vulnerabilities are thus as likely to be global as local. Were foreign intelligence services to penetrate and exploit Internet wiretapping technology, massive surveillance of US citizens, residents, and corporations might follow.

Wiretapping is a security breach, and no one wants to see those breaches, deliberately architected or not.

Used in combination with inexpensive automated search technology, this could lead to an unprecedented compromise of American security and privacy. Of course, Internet protocols govern the entire Internet—

and not a US version—and thus the impact of CALEA on VoIP, were it to succeed, would be international in scope. Across the globe, Internet security and privacy would be put at risk.

The FBI's efforts on CALEA run completely contrary to the US's 220-year history of developing its communication systems.

At present, we're struggling to achieve adequate security on the Internet without intentional security compromises in its design. Although it might one day be possible to incorporate surveillance into packet-switched networks with sufficient security that the overall safety of society is increased rather than decreased, it's hard to see how this could be less difficult than the unfinished task of developing a scalable and economical secure network. At the very least, built-in wiretapping would require secure communications of its own to carry the intercepted information to the customers for which it's collected.

This problem is made worse by the unreasonable effectiveness of the Internet as a communications channel. Building surveillance capabilities into the Internet infrastructure, and not into the application endpoints, would expose to eavesdropping not only current applications, but also future ones, including, for example, the billions of small devices such as radio-frequency identification (RFID) tags and sensors that communicate via the Internet. The concern expressed earlier that security holes built into the Internet for wiretapping that are used in combination with inexpensive automated search technology could lead to serious security breaches applies here as well.

Over the past several years, the US government sought improvements in civilian communications infrastructure security even though some of those improvements were likely to impede law enforcement investigations. Intelligence agencies clearly supported the shift, which found that the advantages provided to society through increased information security outweighed the disadvantages to intelligence and law enforcement. In 2000, the US Department of Commerce relaxed its cryptographic export-control regulations, which simplified the deployment of communications security in commercial equipment. This action marked a substantial change in direction on the civilian sector's use of strong cryptography. Similarly, in recent years, the US government, instead of restricting the use of strong cryptography, has encouraged several cryptographic efforts, including the development of the 128-bit Advanced Encryption Standard and the deployment of Elliptic Curve Cryptosystems.

These changes don't mean that Internet communications can't be wiretapped. The Internet's insecurity is well known, and few communications are routinely protected (for example, encrypted end to end). As the IETF Network Working Group observed, "the use of existing network features, if deployed intelligently, provide extensive opportunities for wiretapping."[23] But exploiting current insecurities and actually building them into Internet protocols have significantly different effects on society's communications security. I'm arguing against the latter; I take no issue with the former.

From the very early days of the republic, the US has treated communications as something "of the people, for the people, and by the people." The US Postal Act of 1792 established two fundamental principles: privacy of the mails—postal officials weren't allowed to open mail unless it was undeliverable—and low rates for newspapers, thereby encouraging the dissemination of political information. In these two decisions, the US acted very differently from Britain and France, which neither guaranteed the privacy of the mails nor encouraged the use of the mails for political communication. Indeed, in Europe, the postal service was a system of government surveillance. By contrast, the US Post Office was seen as a facilitator of democracy rather than a controller of the people and, as a result, it was one of the few strong federal institutions established in the nascent US.[24] A bedrock reason for the growth of telecommunications in the US has been the privacy afforded to communications. This spawned trust in the use of communication systems and a growing dependence on them.[24] The FBI's efforts on CALEA run completely contrary to the US's 220-year history of developing its communication systems.

The attempt to apply CALEA to VoIP poses much risk to the US economy through the potential loss of corporate information, to US national security through the provision of cost-effective massive intelligence gathering, and to privacy and thus the freedom of US citizens.

Society has seen such risks before. In 1999, a report prepared for the European Parliament revealed that the US—as part of a surveillance program known as Echelon, conducted jointly with the United Kingdom, Australia, Canada, and New Zealand—was targeting commercial communication channels.[25] In response, European governments decided to liberalize their cryptographic export-control policy, even though the US had pressed for tighter controls on cryptographic exports. (The US, in part so as not to lose trade to Europe,

liberalized its cryptographic export-control policies shortly afterward.[26])

To law enforcement, it might seem obvious that wiretap laws should automatically be updated with each change in communications technology. Looking at the issues more broadly, this is not a clear proposition. Wiretap laws were passed at a particular time to satisfy a particular set of problems. As technology and society change, so must laws. Society's security needs aren't enhanced by requiring that VoIP implementations be developed as CALEA-enabled, and CALEA requirements applied to the Internet are likely to cause serious harm to security, industrial innovation, and the political efforts in the war against radical terrorists. Applying CALEA to VoIP is likely to decrease, rather than increase security. Security requirements should follow the medical profession's Hippocratic oath: "First, do no harm." The proposed CALEA requirements don't pass this test, and shouldn't be approved. □

Acknowledgments

This article grew out of an invited talk at the 2004 CRYPTO meeting. Sections of this article appeared in the conference proceedings[27] and are reprinted here with the permission of the International Association for Cryptologic Research. In addition, I've been greatly influenced by discussions with my colleague Whitfield Diffie.

References

1. J. Mintz, "Intelligence Community in Breach with Business," *Washington Post,* 30 Apr. 1992, p. A8.
2. B. Schneier and D. Banisar, *The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance*, John Wiley & Sons, 1997.
3. *Communications Assistance for Law Enforcement Act*, Pub. L. No. 103–414, 108 Stat. 4279, United States of America, 1994 (codified as amended in 18 US Code and 47 US Code Section 229, 1001–1010, 1021).
4. *Federal Register*, vol. 70, no. 197, 13 Oct. 2005, p. 59664.
5. S. Dash, R. Schwartz, and R. Knowlton, *The Eavesdroppers,* Rutgers Univ. Press, 1959, p. 23.
6. *Olmstead v. United States*, vol. 277, US Supreme Court, p. 438, 1928.
7. *Nardone v. United States*, vol. 302, US Supreme Court, p. 379, 1937, and vol. 308, US Supreme Court, p. 338, 1939.
8. *Charles Katz v. United States*, vol. 389, US Supreme Court, p. 347, 1967.
9. A. Theoharis and J. Cox, *The Boss: J. Edgar Hoover and the Great American Inquisition*, Temple Univ. Press, 1988.
10. US Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Intelligence Activities and the Rights of Americans, Final Report, Book II*, report 94-755, 1976.
11. A. Charns, *Cloak and Gavel; FBI Wiretaps, Bugs, Informers, and the Supreme Court*, Univ. of Illinois Press, 1992.
12. The President's Commission on Law Enforcement and the Administration of Justice, *The Challenge of Crime in a Free Society*, US Government Printing Office, 1967.
13. US House of Representatives, Committee on the Judiciary, Subcommittee no. 5, *Anti-Crime Program*, Hearings on HR 5037, 5038, 5384, 5385, and 5386, Mar. 15, 16, 22, 23, Apr. 5, 7, 10, 12, 19, 20, 26, and 27, 1967, 90th Congress, 1st Session, 1967.
14. Congressional Quarterly Weekly, vol. 26, 19 July 1968.
15. Omnibus Safe Streets and Crime Control Act. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90–351, United States of America, codified as amended in 18 US Code Section 2510–20, 1968.
16. *United States v. United States*, District Court for the Eastern District of Michigan et al, vol. 407, US Supreme Court, p. 297, 1972.
17. Foreign Intelligence Surveillance, US Code Title 50, chapter 35, sec. 1805(a)(3)(A).
18. M. Scheuer, *Imperial Hubris: Why the West Is Losing the War on Terror*, Brassey's, 2004.
19. National Commission on Terrorist Attacks upon the US, *The 9/11 Commission Report,* W.W. Norton, 2004.
20. P. Heymann, *Terrorism in America: A Commonsense Strategy for a Democratic Society*, MIT Press, 1998.
21. J.H. Saltzer, D.P. Reed, and D.D. Clark, "End-to-End Arguments in System Design," *ACM Trans. Computer Sys.,* vol. 2, no. 4, 1984, pp. 277–288.
22. M. Blumenthal and D. Clark, "Rethinking the Design of the Internet: The End to End Arguments vs. the Brave New World," *ACM Trans. Internet Tech.,* vol. 1, no. 1, 2001, pp. 70–109.
23. Network Working Group, *IETF Policy on Wiretapping,* RFC 2804, May 2000; www.faqs.org/rfcs/rfc2804.html.
24. P. Starr, *The Creation of the Media,* Basic Books, 2004.
25. D. Campbell, "Interception 2000: Development of Surveillance Technology and Risk of Abuse of Economic Information," Report to the Director General for Research of the European Parliament, Luxembourg, Apr. 1999.
26. US Department of Commerce, Bureau of Export Administration: 15 CFR Parts 734, 740, 742, 770, 772, and 774, Docket No. RIN: 0694-AC11, Revisions to Encryption Items, 14 Jan. 2000.
27. S. Landau, "Security, Liberty, and Electronic Communications," *Advances in Cryptology: CRYPTO 2004,* Matt Franklin, ed., Springer-Verlag, pp. 355–372.

Susan Landau *is a distinguished engineer at Sun Microsystems Laboratories, where she works on security, cryptography, and policy, including digital-rights management and surveillance issues. She is coauthor with Whitfield Diffie of* Privacy on the Line: The Politics of Wiretapping and Encryption *(MIT Press, 1998). Landau has a BA from Princeton, an MS from Cornell, and a PhD from MIT. She is a member of the National Institute of Standards and Technology's Information Security and Privacy Advisory Board and a member of the editorial board of* IEEE Security and Privacy. *Landau is an AAAS fellow. Contact her at susan.landau@sun.com.*