



BRAVE NEW WORLD OF WIRETAPPING

As telephone conversations have moved to the Internet, so have those who want to listen in. But the technology needed to do so would entail a dangerous expansion of the government's surveillance powers

By Whitfield Diffie and Susan Landau

As long as people have engaged in private conversations, eavesdroppers have tried to listen in. When important matters were discussed in parlors, people slipped in under the eaves—literally within the “eavesdrop”—to hear what was being said. When conversations moved to telephones, the wires were tapped. And now that so much human activity takes place in cyberspace, spies have infiltrated that realm as well.

Unlike earlier, physical frontiers, cyberspace is a human construct. The rules, designs and investments we make in cyberspace will shape the ways espionage, privacy and security will interact. Today there is a clear movement to give intelligence activities a privileged position, building in the capacity of authorities to intercept cyberspace communications. The advantages of this trend for fighting crime and terrorism are obvious.

The drawbacks may be less obvious. For one thing, adding such intercept infrastructure would undermine the nimble, bottom-up structure of the Internet that has been so congenial to business innovation: its costs would drive many small U.S. Internet service providers (ISPs) out of business, and the top-down control it would require would threaten the nation's role as a leader and innovator in communications.

Furthermore, by putting too much emphasis on the capacity to intercept Internet communications, we may be undermining civil liberties. We may also damage the security of cyberspace and ultimately the security of the nation. If the U.S. builds extensive wiretapping into our communications system, how do we guarantee that the facilities we build will not be misused? Our police and intelligence agencies, through corruption or merely excessive zeal, may use them to spy on Americans in violation of the U.S. Constitution. And, with any intercept capability, there is a risk that it could fall into the wrong hands. Criminals, terrorists and foreign intelligence services may gain access to our surveillance facilities and use them against us. The architectures needed to protect against these two threats are different.

Such issues are important enough to merit a broad national debate. Unfortunately, though, the public's ability to participate in the discussion is impeded by the fog of secrecy that surrounds all intelligence, particularly message interception (“signals intelligence”).

A Brief History of Wiretapping

To understand the current controversy over wiretapping, one must understand the history of communications technology. From the devel-

KEY CONCEPTS

- The advent of computer-based telephone switches and the Internet has made it more difficult for the government to monitor the communications of criminals, spies and terrorists.
- Federal agencies want Internet companies to comply with the same wiretapping requirements that apply to telecommunications carriers. This proposal, though, may stifle Internet innovation.
- Furthermore, the new surveillance facilities might be misused by overzealous government officials or hijacked by terrorists or spies interested in monitoring U.S. communications.

—The Editors

opment of the telephone in the 19th century until the past decade or two, remote voice communications were carried almost exclusively by circuit-switched systems. When one person picked up the phone to call another, one or more telephone switches along the way would connect their wires so that a continuous circuit would be formed. This circuit would persist for the duration of the call, after which the switches would disconnect the wires, freeing resources to handle other calls. Call switching was essentially the only thing that telephone switches did. Other services associated with the telephone—call forwarding and message taking, for example—were handled by human operators.

Wiretapping has had an on-and-off legal history in the U.S. The earliest wiretaps were simply extra wires—connected to the line between the telephone company's central office and the subscriber—that carried the signal to a pair of earphones and a recorder. Later on, wiretaps were installed at the central office on the frames that held the incoming wires. At first, the courts held that a wiretap does not constitute a search when it involves no trespass, but over time that viewpoint changed. In 1967 the U.S. Supreme Court decided in the case of *Katz v. United States* that the interception of communications is indeed a search and that a warrant is required. This decision prompted Congress in 1968 to pass a law providing for wiretap warrants in criminal investigations. But Congress's action left the use of wiretapping for foreign intelligence in legal limbo. Congressional investigations that followed the 1972 Watergate break-in uncovered a history of presidential operations that had employed and, as it turned out, abused the practice, spying on peaceful, domestic political organizations as well as hostile, foreign ones. So, in 1978, Congress passed the Foreign Intelligence Surveillance Act (FISA), which took the controversial step of creating a secret federal court for issuing wiretap warrants.

Most of the surveillance of communications for foreign intelligence purposes lay outside the scope of the wiretapping law, because this activity had primarily involved the interception of radio signals rather than physical intrusions into phone systems. (When operating in other countries, American intelligence services could not place wiretaps on phone lines as easily as they could in the U.S.) Another important distinction between domestic and foreign communications surveillance is scale: inside the U.S., wiretapping has traditionally been regarded as an extreme

How do we guarantee that the communications surveillance facilities we build will not be misused?

investigative technique, something to be applied only to very serious crimes. Outside the country, though, the interception of communications is big business. The National Security Agency (NSA) spends billions of dollars every year intercepting foreign communications from ground bases, ships, airplanes and satellites.

But the most important differences are procedural. Within the U.S. the Fourth Amendment to the Constitution guarantees the right of the people to be free from "unreasonable searches and seizures." The logic of a "reasonable" search is that law-enforcement officers must make an unprivileged observation (that is, one that does not invade the suspect's privacy) whose results give them "probable cause" with which they can approach the courts for a search warrant. What they are not permitted to do, in either physical searches or wiretaps, is to search first and then use what they find as evidence that the search was legitimate. This procedure, however, is exactly what intelligence agents do, except that they usually do not employ their results to prosecute criminals. An intelligence officer relies on professional judgment and available information to make the decision to spy on a foreign target; the operation will then be judged as a success or failure depending on what intelligence was obtained and what resources were expended.

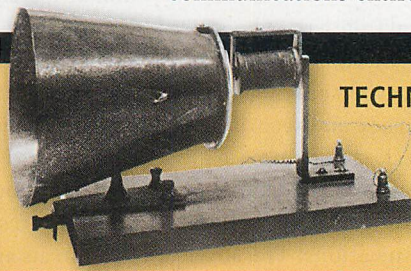
The rules established in FISA make three fundamental distinctions: between "U.S. persons" (citizens, legal residents and American corporations) and foreigners; between communications inside and outside the U.S.; and between wired and wireless communications. Briefly, wired communications entirely within the U.S. are

[MILESTONES]

1876: Alexander Graham Bell invents the telephone.

1875

TECHNOLOGY



1900

1890s: Law-enforcement agencies begin tapping wires on early telephone networks.

A History of Listening In

As the technology of voice communications has advanced, government surveillance has raised many legal issues.

LAW AND POLICY

POLICE HEAD'S TESTIMONY

Wire Spying a Necessity to Detect Crime Here, He Says.

MAYOR CHARGES TREACHERY

Accuses Thompson Committee of Harassing Federal Authorities by Disclosures.

New York Times, May 20, 1916

BETTMAN/CORBIS (telephone receiver), NEW YORK TIMES, PAGE 1, MAY 20, 1916 (newspaper), ANGEL FRANCO AP Photo (Bell Labs sign)

protected—intercepting them requires a warrant. But radio communications that include people outside the country are protected only if the signal is intercepted in the U.S. and the government's target is a particular, known U.S. person who is in the country at the time.

Until recently, whenever the FISA rules applied, they imposed a burden similar to that imposed by ordinary criminal law. To seek a warrant, an intelligence agency had to specify a particular location, telecommunications channel or person and explain why the target should be subject to surveillance. Operating "foreign intelligence-style," intercepting communications and then using the recorded conversations to justify the interception, was not permitted.

Almost accidentally, the rules set by FISA included an important loophole that Congress had intended to be only temporary: radio communications involving parties who were not U.S. persons could be intercepted from inside the U.S. without warrants. At the time FISA was passed and for many years thereafter, the radio exemption was a great boon to the intelligence community. Satellite radio relays had revolutionized international communications in the 1960s and 1970s and carried most of the phone calls entering and leaving the country. Radio communications that were partly or completely among parties outside the U.S. were legally and physically vulnerable to interception by NSA antennas at places such as Yakima, Wash., and Vint Hill Farms in Virginia.

In the 1970s a new transmission medium emerged as an alternative for long-haul communications. Optical fibers—long, thin strands of

MINIMIZATION

One of the important procedural differences between law-enforcement wiretapping and surveillance for foreign intelligence lies in the practice of minimization: avoiding the collection of communications other than the targeted ones. A wiretapped phone line, for example, may be used by several people, some of whom are not the targets of the investigation.

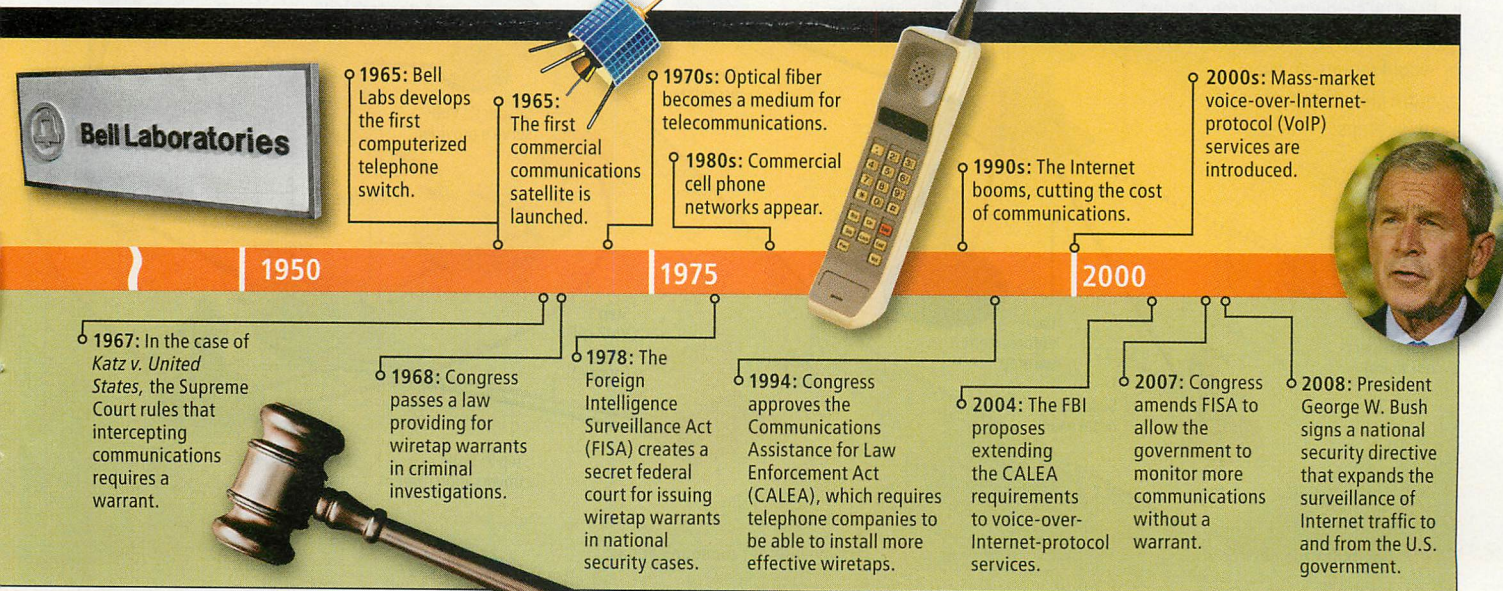
U.S. law requires the police to listen to a tapped conversation at the same time they record it and to stop the surveillance when the subjects are not discussing criminal activities.

In foreign intelligence gathering, the minimization rules are generally not so rigid, but because so many signals can be intercepted and analyzed, far more traffic must be discarded as irrelevant.

glass that carry signals via laser light—offered great advantages in communicating between fixed locations. Fiber lines have tremendous capacity; they are not plagued by the quarter-second delay that slows satellite relays; they are intrinsically more secure than radio; and, for a combination of technical and business reasons, they have become very cheap. From the 1990s onward, the vast majority of communications from one fixed location to another have moved by fiber. Because fiber communications are "wired," U.S. law gives them greater protection. The intelligence community could not intercept these communications as freely as they could radio traffic, and the FISA rules began to chafe.

A particularly sensitive issue for intelligence agencies was the so-called transit traffic. Some 20 percent of the communications carried on U.S. networks originate and terminate outside the country, moving between Europe, Asia and Latin America. Transit traffic is not a new phenomenon; it was already present in the satellite era. But under FISA rules, the interception of fiber communications at points inside the U.S. required a warrant. This requirement upset the standard processes of intelligence agents, who were unaccustomed to seeking probable cause before initiating surveillance.

At about the same time, computer-based switching systems began to replace the traditional electromechanical switches in U.S. telephone networks. This computerization paved the way for services such as automated call forwarding and answering systems, which unintentionally but effectively bypassed standard wiretapping techniques.



Suppose that a caller to a wiretapped phone left a message with an answering service provided by the telephone company. If the target of the investigation checked his messages from a phone other than his own, the communication would never travel over the tapped line and thus would not be intercepted.

Congress responded in 1994 with the Communications Assistance for Law Enforcement Act (CALEA), which requires telecommunications companies to make it possible for the government to tap all the communications of a targeted subscriber no matter what automated services the subscriber uses. In addition to mandating

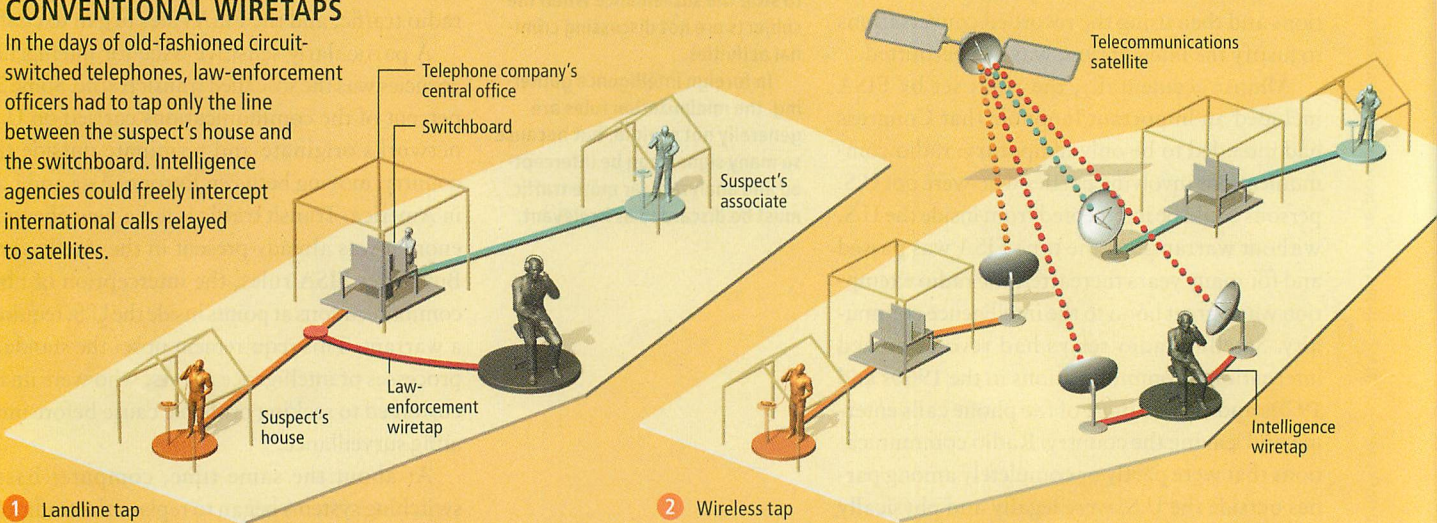
[THE BASICS]

Then and Now: Surveillance Gets Complicated

Monitoring voice communications has grown more technically challenging in recent years, requiring more simultaneous wiretaps.

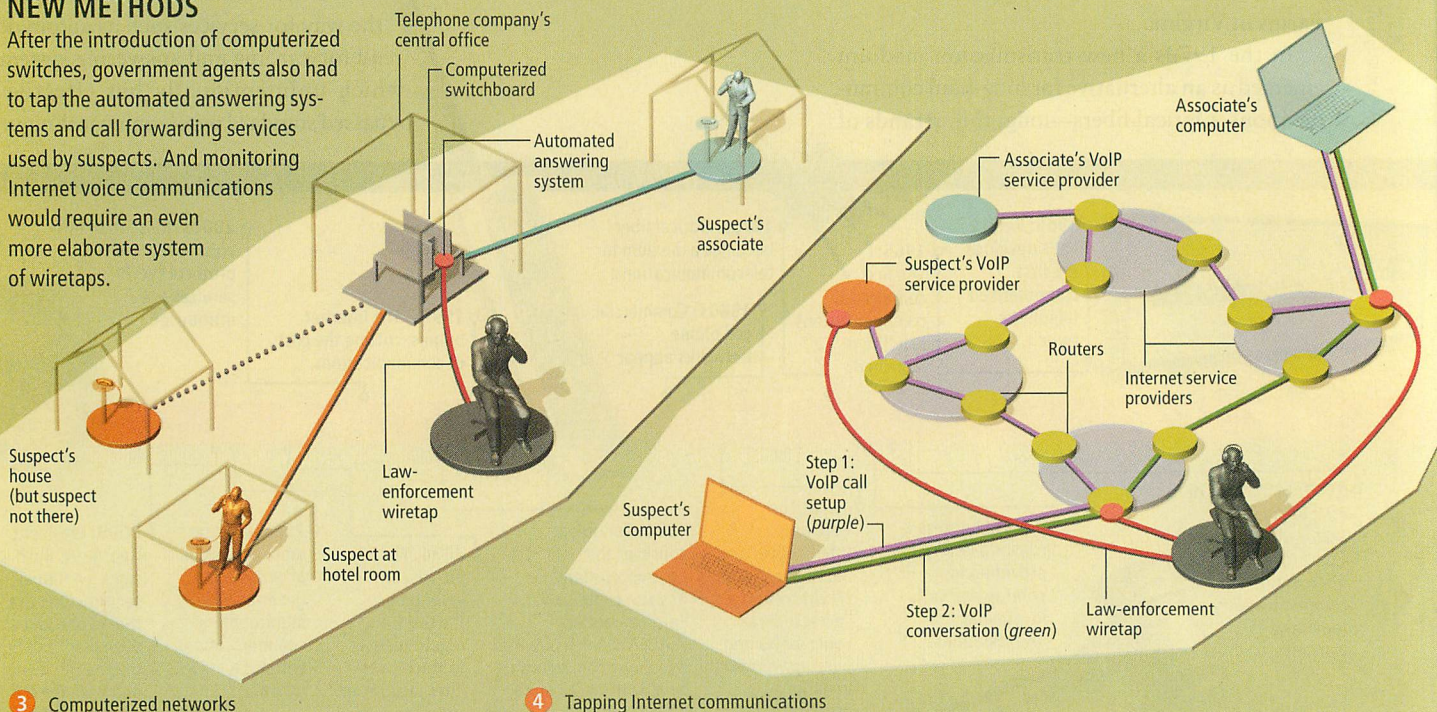
CONVENTIONAL WIRETAPS

In the days of old-fashioned circuit-switched telephones, law-enforcement officers had to tap only the line between the suspect's house and the switchboard. Intelligence agencies could freely intercept international calls relayed to satellites.



NEW METHODS

After the introduction of computerized switches, government agents also had to tap the automated answering systems and call forwarding services used by suspects. And monitoring Internet voice communications would require an even more elaborate system of wiretaps.



an improvement in the quality of information that can be obtained from wiretaps, CALEA obliged telecommunications carriers to be able to execute far more simultaneous wiretaps than had previously been possible.

Tapping the Net

CALEA was passed just as large numbers of people began using the Internet, which employs a communications method that is entirely different from circuit-switched telephony. Internet users send information in small packets, each of which carries a destination address and a return address, just like a letter in the postal system. With circuit switching, a brief telephone call incurs the same setup costs as a long one, so making a call to send only a few words is uneconomical. But on a packet-switched network, short messages are cheap and shorter messages are cheaper. Web browsing is possible because Internet connections can be used briefly and discarded. Each time you click on a Web link, you establish a new connection.

In the era of circuit-switched communications, wiretapping worked because telephone instruments, numbers and users were bound closely together. A telephone was hard to move, and a new telephone number was hard to get. An organization's messages moved on the same channels for long periods, so it was easy to intercept them repeatedly. Computerized switching and the Internet have made surveillance much more challenging. Today people can easily get new telephone numbers as well as e-mail addresses, instant messaging handles and other identifiers. And the advent of voice-over-Internet protocol (VoIP), the standard that allows the transmission of voice communications over packet-switched networks, has further decentralized control of the communications infrastructure. In a VoIP system such as the popular Skype service, for example, the setting up of phone calls and the transmission of traffic are entirely separate.

If CALEA, as interpreted literally, were applied to decentralized VoIP services, the provider would be required to intercept targeted customers' phone calls and relay them to the government but might be totally incapable of complying with such a demand. Consider a typical VoIP call running between the laptop computers of two people, both of whom are traveling. Alice initiates the call from a lounge at O'Hare airport in Chicago, and Bob receives it at a hotel bar in San Francisco. The VoIP provider's role in the process is limited: it discovers the

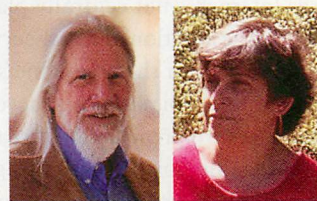
Internet protocol (IP) addresses through which Alice and Bob are connected and communicates each person's address to the other's computer. After the setup is completed, the VoIP provider plays no further role. Instead the actual voice conversation is carried by the Internet service providers (ISPs) through which Alice and Bob access the Internet, together with other Internet carriers to which those ISPs are connected.

In this environment a government agency might have to serve wiretap warrants on many telecommunications carriers just to monitor a single target. Suppose we imagine a CALEA-style intercept regime that could capture a VoIP call. It must begin with an order to the VoIP provider targeting either Alice or Bob. When law-enforcement agents receive word from the provider that the target is engaged in a call, they must consider the IP addresses of Alice and Bob and send an intercept warrant to one or more ISPs at which the call can be intercepted. The ISPs must be prepared to accept, authenticate and implement the warrant in real time. One problem with this scenario is that only ISPs in the U.S. (and possibly some in cooperating countries) would be required to honor the warrant. A more serious difficulty is the massive security problem that such an arrangement would present. Anyone who could penetrate an ISP's wiretap function would be able to spy on its subscribers at will.

CALEA recognized the difference between traditional telephony and the Internet and exempted the Internet, referred to as "information services," from the provisions of the new law. Yet in 2004, despite that distinction, the U.S. Department of Justice, the Federal Bureau of Investigation and the U.S. Drug Enforcement Administration responded to the challenge of monitoring Internet communications by proposing that providers of broadband Internet access be required to comply with the CALEA requirements. The Federal Communications Commission and the courts have so far supported law enforcement in extending CALEA to "interconnected VoIP" (the form most like traditional telephony), relying on a provision of CALEA that refers to services that are a "substantial" replacement for the telephone system. This proposal, if adopted, would be the first step on a road leading to dangers not present in conventional wiretapping.

In particular, the government's actions threaten the continued growth of the Internet, which has become a hotbed of innovation as a consequence of its distributed control and loose con-

[THE AUTHORS]



Whitfield Diffie began his career in security as the inventor of the concept of public-key cryptography. In the 1990s he turned his attention to public policy and played a crucial role in opposing government key-escrow proposals and restrictive regulations on the export of products incorporating cryptography. He is now chief security officer at Sun Microsystems and is studying the impact of Web services and grid computing on security and intelligence.

Susan Landau is a distinguished engineer at Sun Microsystems Laboratories, where she works on security, cryptography and policy, including surveillance and identity-management issues. Landau had previously been a faculty member at the University of Massachusetts Amherst and Wesleyan University, where she worked on algebraic algorithms.

nectivity. Unlike a telephone carrier's network, the Internet is not centrally planned and managed. The addition of a new service, such as call forwarding, in the telephone system typically takes years of planning and development. But an Internet entrepreneur can start a new business in a garage or dorm room, using nothing but a home computer and a broadband connection. If law enforcement succeeds in mandating interception facilities for every Internet carrier, the industry as a whole could be pushed back into the procrustean bed of conventional telecommunications. To incorporate extensive surveillance capabilities, new Internet services would have to be developed in long cycles dependent on federal approval. In a century in which the great opportunities lie in information-based businesses, Americans must do everything possible to foster innovation rather than stifling it. If we do not, we may fall behind countries that follow a different course. Such an outcome would represent a long-term threat to national security.

Another threat is more immediate. Since the collapse of the Soviet Union, no opponent has had the ability to spy on U.S. communications with anything approximating comprehensive coverage. The Soviets had fleets of trawlers patrolling both coasts of the U.S., diplomatic facilities in major American cities, satellites overhead and ground bases such as the Lourdes facility near Havana. Their capabilities in signals intelligence were second to none. In comparison, the current opponents we most fear, such as al Qaeda, and even major nations such as China have no such ability. They are, however, trying to achieve it, and building wiretapping into the Internet might give it to them. Computers would control the intercept devices, and those computers themselves would be controlled remotely. Such systems could be just as much subject to capture as Web sites and personal computers. The government's proposed interception policies must be judged in the light of such vast and uncertain dangers.

Cyberwars

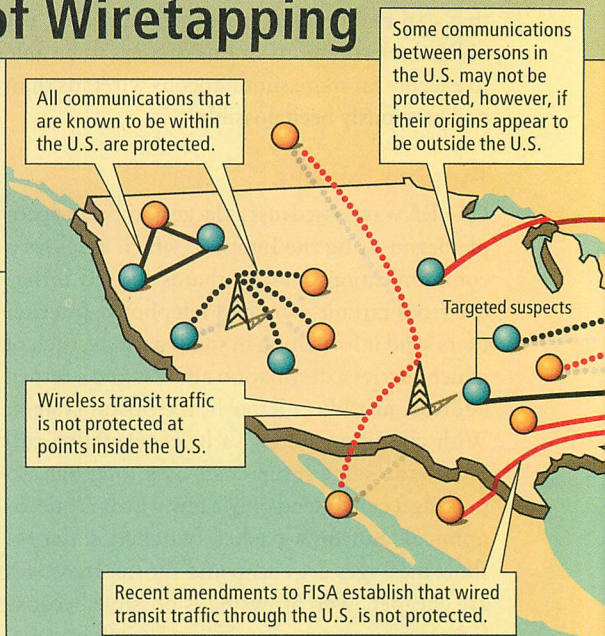
The administration of President George W. Bush recently relaxed some of the 30-year-old restrictions on communications surveillance mandated by FISA. In 2007 Congress, under intense pressure from the White House, passed the Protect America Act (PAA), which amended FISA by expanding the radio exemption to cover all communications. The law provided that any communication reasonably believed to have

[SURVEILLANCE LAW]

Geography of Wiretapping

The Foreign Intelligence Surveillance Act (FISA), amended this year, details which communications are legally protected and which can be monitored without a warrant.

- U.S. person (citizen, legal resident or American corporation)
- Non-U.S. person
- Wired (*solid*)
- ... Wireless (*dashed*)
- Protected communication (wiretap requires a warrant)
- Unprotected communication (can be tapped without a warrant)

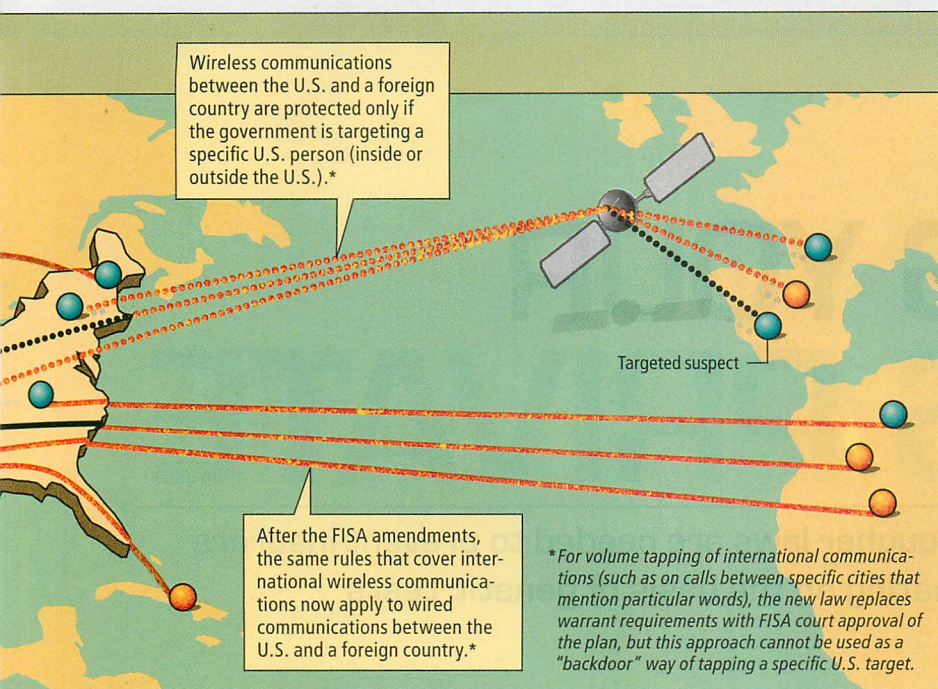


a participant outside the U.S. could be intercepted without a warrant. Given the degree to which business services in the U.S. are being outsourced to overseas providers, the new law made a large fraction of American commercial and personal telecommunications activity subject to monitoring. Congress was sufficiently nervous about this course of action that it provided for PAA to expire in 2008.

This past July, after months of controversy, Congress passed a bill fundamentally expanding the executive branch's wiretapping authority and reducing the FISA court's role in international cases to reviewing the general procedures of a proposed wiretap rather than the specifics of a case. Political debate over the bill, however, did not center on wiretapping authority, as one might expect for a sweeping change. Most attention focused instead on giving retroactive immunity for past illegal wiretapping.

In early 2008 the administration offered a new rationale for expanding communications surveillance: securing the Internet. The current state of Internet security is indeed abysmal. Most computers cannot protect themselves from penetration by malware—software designed to infiltrate and damage computer systems—and a substantial fraction of the computers linked to the Internet are under the control of parties other than their owners. These machines have been surreptitiously captured and organized into “botnets,” whose computing power is then resold in a kind of electronic slave trade. In

Communication is fundamental to our species; privacy of communication is fundamental to both our national security and our democracy.



response to the failure of traditional defensive approaches, President Bush signed a national security directive in January authorizing a Cyber Initiative. Most of the initiative is secret, but its initial move—extensive surveillance of the substantial amount of Internet traffic that moves in and out of the U.S. government—is too sweeping to be concealed. To facilitate the surveillance, the administration plans to reduce the number of connections between government agencies and the Internet from thousands to fewer than a hundred, and that requires changing or retiring thousands of IP addresses. The Cyber Initiative captures the dilemma of signals intelligence perfectly. A system that monitors federal communications for signs of foreign intrusion will also capture all the legitimate communications that Americans have with their government.

The administration is seeking the power to intercept American communications using the same tactics long employed in foreign intelligence gathering—that is, without having to go to the courts for warrants and describe in advance whose communications it intends to intercept. The advocates of expanded surveillance have valid concerns: not only do we face opponents who are not tied to particular nations and can move freely in and out of the U.S., we also have a critical cybersecurity problem. The Internet is swiftly becoming the primary medium for both commercial and government business, as well as the preferred communications method for many individuals. Its security problems are analogous

to having the roads overrun with bandits or the sea-lanes controlled by pirates. Under these circumstances, it is not surprising to find the government seeking to patrol the Internet, just as the nation's police and armed services have patrolled the roads or the high seas in the past.

But policing the Internet, as opposed to securing the computers that populate it, may be a treacherous remedy. Will the government's monitoring tools be any more secure than the network they are trying to protect? If not, we run the risk that the surveillance facilities will be subverted or actually used against the U.S. The security problems that plague the Internet may beset the computers that will do the policing as much as the computers being policed. If the government expands spying on the Internet without solving the underlying computer security problems, we are courting disaster.

The inherent dangers are made worse by the secrecy surrounding the government's initiatives. One casualty of recent approaches to communications interception has been what might be called the two-organization rule. The security of many crucial systems, such as those controlling nuclear weapons, relies on the requirement that critical actions be taken by two people simultaneously. Until recently, federal law mandated a similar approach to wiretapping, allowing the government to issue wiretap orders but requiring the phone companies to install the taps. Under this arrangement, a phone company would be reluctant to act on a wiretap order it suspected was illegal, because its compliance would make it vulnerable to both prosecution and civil liability. Eliminating the role of the phone companies removes an important safeguard. If we follow this course, we may create a regime entirely out of view of Congress, the courts and the press—and perhaps entirely out of control.

The distance our world has moved into cyberspace in the past century is minuscule compared with the distance it will move in the next. We are in the process of building the world in which future humans will live, as surely as the first city dwellers did 5,000 years ago. Communication is fundamental to our species; private communication is fundamental to both our national security and our democracy. Our challenge is to maintain this privacy in the midst of new communications technologies and serious national security threats. But it is critical to make choices that preserve privacy, communications security and the ability to innovate. Otherwise, all hope of having a free society will vanish. ■

MORE TO EXPLORE

Information Privacy Law: Cases and Materials. Second edition. Daniel J. Solove, Marc Rotenberg and Paul Schwartz. Aspen, 2005.

Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP. Steven M. Bellovin, Matt Blaze, Ernest Brickell, Clinton Brooks, Vinton Cerf, Whitfield Diffie, Susan Landau, Jon Peterson and John Treichler. Information Technology Association of America, 2006. Available at www.itaa.org/news/docs/CALEAVOIPreprint.pdf

Privacy on the Line: The Politics of Wiretapping and Encryption. Updated and expanded edition. Whitfield Diffie and Susan Landau. MIT Press, 2007.

More information on communications surveillance issues is available at the Web sites of the Center for Democracy and Technology: www.cdt.org; the Electronic Frontier Foundation: www.eff.org; and the Electronic Privacy Information Center: www.epic.org