# Wiretapping and Other Eavesdropping Devices and Methods

Updated: Oct. 19, 2010

Wiretapping and electronic eavesdropping are virtually as old as the telephone. But the debates over wiretapping have intensified in recent years, as the pressure to fight terrorism after the Sept. 11th attacks and rapid technological change led to an unprecedent expansion of electronic surveillance.

After the attacks in 2001, members of the Bush administration were highly critical of restrictions on surveillance imposed by laws like FISA, the Foreign Intelligence Surveillance Act, which was passed in 1978 after Congressional hearings revealed widespread abuse of government wiretaps.

Portions of the Patriot Act expanded the law's reach to cover terrorism suspects as well as agents of foreign countries. But when President Bush ordered an expanded program of surveillance by the National Security Agency, he decided to bypass the FISA process entirely. When news of these warrantless wiretaps was revealed by The New York Times in 2005, administration officials argued that working within FISA would have been too cumbersome.

In the midst of the presidential campaign in 2008, Congress overhauled the Foreign Intelligence Surveillance Act to bring federal statutes into closer alignment with what the Bush administration had been secretly doing. The legislation essentially legalized certain aspects of the program.

As a senator then, Barack Obama voted in favor of the new law, despite objections from many of his supporters. President Obama's administration now relies heavily on such surveillance in its fight against Al Qaeda. It has also been working to revamp the rules for wiretapping to meet what they see as new technological challenges.

For one thing, the administration wants Congress to require all services that enable communications — including encrypted e-mail transmitters like BlackBerry, social networking Web sites like Facebook and software that allows direct “peer to peer” messaging like Skype — to be technically capable of complying if served with a wiretap order. It is also working want to increase legal incentives and penalties aimed at pushing carriers like Verizon, AT&T, and Comcast to ensure that any network changes will not disrupt their ability to conduct wiretaps.

**Push to Ease Wiretapping Obstacles**

Law enforcement and counterterrorism officials, citing lapses in compliance with surveillance orders, are pushing to overhaul a federal law that requires phone and broadband carriers to ensure that their networks can be wiretapped.

The officials say tougher legislation is needed because some telecommunications companies in recent years have begun new services and made system upgrades that caused technical problems for surveillance. They want to increase legal incentives and penalties aimed at pushing carriers like Verizon, AT&T, and Comcast to ensure that any network changes will not disrupt their ability to conduct wiretaps.

An Obama administration task force that includes officials from the Justice and Commerce Departments, the F.B.I. and other agencies recently began working on draft legislation to strengthen and expand the Communications Assistance to Law Enforcement Act, a 1994 law that says telephone and broadband companies must design their services so that they can begin conducting surveillance of a target immediately after being presented with a court order.

The push to expand the government's leverage over carriers and the 1994 law is the latest example of a dilemma over how to balance Internet freedom with security needs in an era of rapidly evolving — and globalized — technology. The issue has added importance because the surveillance technologies developed by the United States to hunt for terrorists and drug traffickers can be also used by repressive regimes to hunt for political dissidents.

To bolster their case that telecom companies should face greater pressure to stay compliant, security agencies are citing two previously undisclosed episodes in which investigators were stymied from carrying out court-approved surveillance for weeks or even months because of technical problems with two major carriers.

The disclosure that the administration is seeking ways to increase the government's leverage over carriers already subject to the 1994 law comes less than a month after The New York Times reported on a related part of the effort: a plan to bring Internet companies that enable communications — like Gmail, Facebook, Blackberry and Skype — under the law's mandates for the first time, a demand that would require major changes to some services' technical designs and business models.

Under current law, if a carrier meets the industry-set standard for compliance — providing the content of a call or e-mail, along with identifying information like its recipient, time and location — it achieves "safe harbor" and cannot be fined. If the company fails to meet the standard, it can be fined by a judge or the Federal Communication Commission.

But in practice, law enforcement officials say, neither option is ever invoked. When problems come to light, officials are reluctant to make formal complaints against companies because their overriding goal is to work with their technicians to fix the problem.

**Court Challenges**

On March 31, 2010, a federal judge ruled that the National Security Agency's program of surveillance without warrants was illegal, rejecting the Obama administration's effort to keep shrouded in secrecy one of the most disputed counterterrorism policies of former President George W. Bush.

The Obama administration also began an effort to seek sweeping new regulations for the Internet, arguing that their ability to wiretap criminal and terrorism suspects is "going dark" as people increasingly communicate online instead of by telephone. Essentially, officials want Congress to require all services that enable communications — including encrypted e-mail transmitters like BlackBerry, social networking Web sites like Facebook and software that allows direct "peer to peer" messaging like Skype — to be technically capable of complying if served with a wiretap order. The mandate would include being able to intercept and unscramble encrypted messages.

In a 45-page opinion, Judge Vaughn R. Walker, the chief judge of the Federal District Court in San Francisco, ruled that the government had violated a 1978 federal statute requiring court approval for domestic surveillance when it intercepted phone calls of Al Haramain, a now-defunct Islamic charity in Oregon, and of two lawyers representing it in 2004. Declaring

that the plaintiffs had been "subjected to unlawful surveillance," the judge said the government was liable to pay them damages.

The Justice Department had argued that the charity's lawsuit should be dismissed without a ruling on the merits because allowing it to go forward could reveal state secrets. The judge characterized that expansive use of the so-called state-secrets privilege as amounting to "unfettered executive-branch discretion" that had "obvious potential for governmental abuse and overreaching." That position, he said, would enable government officials to flout the warrant law, even though Congress had enacted it "specifically to rein in and create a judicial check for executive-branch abuses of surveillance authority.

The ruling was the second time a federal judge has declared the program of wiretapping without warrants to be illegal. But a 2006 decision by a federal judge in Detroit, Anna Diggs Taylor, was reversed on the grounds that those plaintiffs could not prove that they had been wiretapped and so lacked legal standing to sue.

Several other lawsuits filed over the program have faltered because of similar concerns over standing or because of immunity granted by Congress to telecommunications companies that participated in the N.S.A. program. By contrast, the Haramain case was closely watched because the government inadvertently disclosed a classified document that made clear that the charity had been subjected to surveillance without warrants.

In an earlier court action, in January 2009 the federal intelligence court itself issued a rare public ruling upholding the 2007 law, validating the power of the president and Congress to wiretap international phone calls and intercept e-mail messages without a specific court order, even when Americans' private communications may be involved.

In April 2009, officials revealed that a Justice Department review found that since the passage of the Protecting America Act the NSA intercepted private e-mail messages and phone calls of Americans on a scale that went beyond the broad legal limits established by Congress.

The overcollection problems appear to have been uncovered as part of a twice-annual certification that the Justice Department and the director of national intelligence are required to give to the Foreign Intelligence Surveillance Court on the protocols that the N.S.A. is using in wiretapping. New details also emerged about earlier domestic-surveillance activities, including the agency's attempt to wiretap a member of Congress, without court approval, on an overseas trip.

A report produced by five inspectors-general questioned the program's value, saying that its revelations played a limited role in the F.B.I.'s counterintelligence work and that other methods had produced more timely information. The report also hinted at political pressure in preparing the so-called threat assessments that helped form the legal basis for continuing the classified program