Cato Handbook for Policymakers

CATO INSTITUTE

7TH EDITION

28. Electronic Surveillance

Congress should

- repeal the FISA Amendments Act of 2008;
- conduct a thorough, public investigation of executive branch surveillance activities over the last three decades;
- require individualized warrants for all eavesdropping conducted on U.S. soil unless both ends of a communication are known to be overseas;
- require prior judicial approval of all domestic intercepts, allowing a 72-hour grace period for emergency foreign intelligence intercepts;
- require that foreign intelligence be the purpose of all FISA intercepts and prohibit coordination between law enforcement and intelligence officials in the choice of FISA eavesdropping targets; and
- reverse the Federal Communications Commission's decisions extending the Communications Assistance for Law Enforcement Act to broadband and Internet telephony providers.

The George W. Bush administration pushed relentlessly for broader domestic eavesdropping powers. In the wake of the 9/11 terrorist attacks, the president persuaded Congress to pass the USA Patriot Act, which included numerous provisions expanding domestic spying authority and limiting judicial oversight. He authorized domestic spying programs that were kept secret for several years before they were revealed by whistleblower testimony and media reports. When the programs were brought to light, the Bush administration pressured the Foreign Intelligence Surveillance Court—the secret court created to oversee wiretapping activities—to authorize the programs under existing wiretapping rules. When it reportedly refused, the White House turned to Congress, asking it to weaken

judicial oversight of domestic surveillance activities. Congress complied with the 2008 FISA Amendments Act.

Don't Overestimate Wiretapping

One effect of the noisy debate over domestic wiretapping has been to greatly exaggerate its importance as a crime-fighting tool. Congress prohibited the federal government from engaging in any wiretapping between 1934 and 1968. In 1968, Congress authorized wiretaps for law enforcement purposes that have come to be known as ''Title III'' wiretaps. But the use of these wiretaps in investigations of violent crimes continues to be extremely rare. For example, according to the Federal Bureau of Investigation, 17,034 murders, 91,111 rapes, and 855,088 aggravated assaults were committed in 2006, yet the courts authorized only 119 wiretaps in homicide or assault cases. Criminals committed 12 million property crimes in 2006, but the courts authorized only 20 wiretaps in property crime investigations. The vast majority of Title III law enforcement wiretaps—more than 80 percent—are deployed as part of the drug war, an effort that (as discussed in Chapter 33) creates more problems than it solves.

Details on the use of wiretaps for intelligence-gathering and counterterrorism purposes are not available to the public, so it is difficult to judge how crucial wiretaps are in those efforts. But one thing that can safely be said is that technological changes, including the increased flexibility of communications networks and the growing availability of encryption technologies, are making it easier for everyone—law-abiding citizens and terrorists alike—to evade surveillance. Even the most draconian wiretapping laws are unlikely to reverse that trend. A counterterrorism strategy that relies too heavily on wiretapping is a recipe for failure.

Fortunately, government officials have many options for collecting intelligence that do not rely on wiretaps. They include (as permitted by law) installing bugs, intercepting radio communications, subpoenaing relevant business records, infiltrating groups under investigation, and employing confidential informants. The government should be given as much wiretapping authority as is consistent with the protection of civil liberties, but it would be a serious mistake to sacrifice constitutional protections in a futile effort to make wiretapping as easy as it was four decades ago.

Law enforcement and intelligence officials are—properly—focused on catching criminals and terrorists, and they naturally seek the broadest

possible powers to do their jobs. But in the process, they have a tendency to lose sight of protecting the rights of innocent Americans. Too often, they seek new powers that will only marginally enhance their investigative powers while significantly eroding constitutional rights. That's why judicial oversight is crucial. We *want* law enforcement to seek every possible advantage in their fight against criminals and terrorists. But we also need independent judges to rein them in when they stray beyond the bounds of the Constitution.

Create a New Church Committee

The erosion of judicial oversight during the Bush administration is troubling because history suggests that judicial oversight is a crucial check on the abuse of executive power. In 1976, a Senate committee headed by Sen. Frank Church (D-ID) released a massive report on abuses of power by federal officials during the preceding half century. It found that the Federal Bureau of Investigation, the National Security Agency, and other government agencies had repeatedly violated the privacy of law-abiding citizens, not to mention federal law. Hundreds of nonviolent political activists, celebrities, journalists, labor leaders, and elected officials were subject to illegal wiretaps, bugs, mail openings, and break-ins during the cold war. The investigation was prompted by the Watergate scandal, but the Church Committee found that abuses of power didn't start with Richard Nixon. Every president since Franklin D. Roosevelt had approved unlawful surveillance programs.

Although the details remain wrapped in secrecy, media reports and the testimony of government whistle-blowers suggest that the George W. Bush administration may have broken the law by spying on law-abiding Americans without a warrant. The *New York Times* reported on one warrantless spying program in December 2005. In March 2006, a retired AT&T technician declared under oath that AT&T had given the NSA unfettered access to its customers' voice and data traffic as that traffic passed through its switching centers in San Francisco and other cities. A May 2006 *USA Today* article revealed another potentially illegal spying program; this one collected the domestic calling records of Americans and attempted to use data-mining software to detect suspicious calling patterns.

The Bush administration took the position that these actions were within the president's inherent authority or were permitted by the Authorization for Use of Military Force passed by Congress. These positions are inconsistent with the history, structure, and text of those documents.

Congress cannot craft sensible new eavesdropping rules until it has a clear picture of the government's current domestic spying activities. With the end of the George W. Bush administration, the time is ripe for another in-depth congressional investigation of potentially illegal surveillance by the executive branch. Although Bush administration activities should be a major focus, the investigation should not focus solely on the last eight years. Instead, it should start where the Church Committee left off and investigate domestic spying activities undertaken since the mid-1970s.

Restore FISA Safeguards

In 1978, Congress passed the Foreign Intelligence Surveillance Act, which, for the first time, permitted the use of domestic wiretaps for intelligence-gathering purposes. FISA required judicial oversight of these spying activities, requiring the executive branch to show probable cause that the target was an ''agent of a foreign power,'' and that ''the purpose'' of the surveillance was foreign intelligence. To ensure that this new, more permissive wiretapping regime was not used for ordinary criminal investigations, the law restricted coordination between officials conducting FISA wiretaps and federal agents involved in ordinary law enforcement. Finally, recognizing that national security could occasionally require the initiation of wiretapping before there was time to seek a court order, FISA created an emergency process whereby the government could begin spying immediately and seek court authorization within 72 hours.

Unfortunately, between 2001 and 2008, Congress crippled the system of judicial oversight it had carefully constructed in 1978. Whereas FISA had originally required that foreign intelligence be ''the purpose'' of FISA surveillance, the 2001 Patriot Act required that foreign intelligence be only ''a significant purpose'' of surveillance. The courts interpreted this as a green light for coordination between intelligence and law enforcement—even in ordinary criminal cases. That's troubling because the rules for FISA warrants do not require the government to show probable cause that the target has broken the law. Law enforcement and intelligence officials need flexibility to share information about ongoing terrorism investigations, but the FISA process should not be used to spy on Americans for ordinary law enforcement purposes. (The so-called wall between criminal and intelligence investigators that supposedly prevented full pursuit of the 9/11 terrorists was a product of bureaucratic incompetence—not the bar on using FISA wiretaps for ordinary crime investigations.)

This danger was greatly enhanced in 2008 when Congress passed the FISA Amendments Act. It allows the government to intercept the international calls of Americans without an individualized warrant. The government need only submit a ''certification'' to the FISA court describing the general parameters of an eavesdropping program. And the government can begin wiretapping immediately, then drag out the judicial review process for as long as four months.

The new rules include a few provisions ostensibly designed to limit abuses, but those limitations are little more than symbolic. The legislation prohibits the ''targeting'' of specific Americans and requires that the government adopt ''minimization'' procedures. However, the legislation places no limits on the breadth of interceptions and places few restrictions on the kinds of information that can be retained and the things that can be done with it. Moreover, it specifically provides that the government is not required to ''identify the specific facilities, places, premises, or property'' at which interceptions will occur. The details of which communications facilities will be tapped and whose communications will be intercepted will be transmitted directly from the government to telecommunications companies. As a consequence, the judge nominally overseeing the eavesdropping will often lack the information necessary to verify that the law is being followed.

Limit Data Mining

Each of these changes is problematic when viewed in isolation; together, they add up to something even more troubling: the de facto legalization of indiscriminate, or ''dragnet,'' surveillance of Americans' international calls. It appears that the government could, for example, intercept all communications between a particular American city and the Middle East, sifting the traffic for particular words, phrases, or voiceprints. Under such a program, thousands of innocent Americans could have their communications intercepted, reviewed by human analysts, and passed on to other federal agencies, all without meaningful court oversight.

Some advocates contend that such expanded powers are essential to the fight against terrorism. They argue that only by collecting reams of data and feeding it into sophisticated pattern-matching algorithms—often called ''data mining''—can we detect terrorist plots in time for law enforcement officials to foil them.

This argument greatly exaggerates the utility of data-mining technologies for counterterrorism efforts. Data-mining techniques work well in

business applications such as credit card fraud detection and direct-mail marketing because businesses have thousands of data points with which to tune their algorithms. In contrast, the number of terrorist attacks or instances of terrorism planning on American soil has (thankfully) been far too small to compile a useful profile of the ''typical'' terrorist. Even the best commercial data-mining applications have a high ''false-positive'' rate. Using the same algorithms on the terrorist-detection problem would swamp federal agents with the names of innocent Americans. Investigators need fewer leads of higher quality, not many leads of low quality.

Recent history bears this out. In summer 2001, U.S. officials were aware that two men linked to the bombing of the USS *Cole* were in the country. They were not sought, and they became two of the 9/11 hijackers. Casting a broader net for suspects would not have aided the effort to apprehend these two; it would only have given investigators more false leads and distracted them from the real terrorists. However, the British government successfully thwarted a liquid explosives plot in August 2006 using traditional police practices, including an undercover British agent. Dragnet surveillance and data mining would have simply overwhelmed an already overworked law enforcement community. This is a case where liberty and security are not in tension: prohibiting dragnet surveillance and data mining will enhance civil liberties while focusing anti-terrorism efforts. Congress should require individualized warrants for domestic spying even if that precludes the use of these techniques.

Repeal the FISA Amendments Act

Some of the worst provisions of the FISA Amendments Act are due to expire at the end of 2013. However, the nation cannot afford to go that long without adequate judicial oversight. These provisions should be repealed before then. After it has completed its investigation of recent executive eavesdropping activity, Congress should enact more comprehensive legislation that updates surveillance law in a way that will prevent the recurrence of any abuses uncovered by the investigation. At a minimum, it should include individualized warrants, judicial review before the start of eavesdropping (or, in emergency cases, no more than 72 hours after), and restrictions on the use of FISA wiretaps for ordinary law enforcement purposes.

Reform CALEA

In the early 1990s, the FBI began to complain that technological changes in the phone system were impeding wiretaps. Civil liberties groups argued

that these complaints were exaggerated. But in 1994, Congress enacted the Communications Assistance for Law Enforcement Act, which required telecom companies to build eavesdropping capabilities into new telephone switches. In 2005, the FCC extended these requirements to broadband service providers and any voice-over-Internet-protocol (VoIP) providers that interconnect with the traditional telephone network.

Deregulate VoIP

Congress should overrule the FCC's ruling because the Internet differs from the telephone network in ways that make complying with CALEA regulations far more burdensome. With traditional landline telephone service, there is invariably a specific company with the ability to intercept all calls to and from a given phone number. Because of the Internet's decentralized architecture, the same is not true of Internet communications. Communications between two VoIP users may travel directly from the sender to the receiver without passing through any servers owned by the software developer. And because someone can log on to the Internet from anywhere in the world, it will often be impossible to predict where to place a wiretap to intercept a given user's calls.

There are two ways that the developers of VoIP applications can comply with CALEA regulations. One is to design their software to use a central server. That would make the software more expensive to deploy (because servers cost money) and would probably degrade its performance. It would also be inconsistent with Congress's intent that vendors not be forced to fundamentally redesign their products to comply with CALEA.

The other option is to add a ''back door'' to VoIP software that remotely activates an eavesdropping mode when asked to do so by the courts. That solution would create at least two problems. First, there is a risk that the back door could be discovered and exploited by unscrupulous third parties to eavesdrop on unsuspecting users' telephone calls. Second, sophisticated users could detect such eavesdropping by monitoring the network traffic being generated by the software. If the conversation were being transmitted to a third party, it would tip off tech-savvy criminals that they were being monitored.

Both these approaches suffer from an additional weakness: they would almost certainly be discovered and publicized. Because the Internet is a global network, there will always be non-CALEA-compliant communications software available for those who know where to look. Given that criminals and terrorists will gravitate toward this software, there is little

point in subjecting only some VoIP providers to CALEA rules. Accordingly, Congress should overrule the FCC and explicitly exempt all Internet-based applications—including VoIP—from CALEA's requirements.

Deregulate Broadband

Congress should do the same for broadband providers. The Internet is still a rapidly changing medium, and requiring every Internet service provider to build eavesdropping into its devices creates a barrier to entry for smaller firms. It is important to remember that exempting ISPs from CALEA would not excuse them from assisting in wiretaps. Providers would still be required to respond to court orders by offering law enforcement technical assistance and access to their facilities. That's how all wiretaps worked before 1994, and in most cases, it will allow law enforcement to obtain a suspect's Internet traffic. But it is overkill to require the installation of eavesdropping equipment in every networking closet in America. Congress should overrule the FCC and make clear that all Internet-based service providers are exempt from CALEA regulations.

Suggested Readings

Diffie, Whitfield, and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption.* Cambridge, MA: MIT Press, 2007.

Healy, Gene, and Timothy Lynch. ''Power Surge: The Constitutional Record of George W. Bush.'' Cato Institute white paper, May 1, 2006.

Jonas, Jeff, and Jim Harper. ''Effective Counterterrorism and the Limited Role of Predictive Data Mining.'' Cato Institute Policy Analysis no. 584, December 11, 2006.

Lee, Timothy B. ''The New FISA Compromise: It's Worse than You Think.'' *Ars Technica*, July 7, 2008. http://arstechnica.com/articles/culture/fisa-compromise.ars.

—Prepared by Timothy B. Lee