Legalize it?
Should the law make room for warrantless wiretapping? The debate has already begun.

By Emily Bazelon | February 19, 2006

WHEN NEWS of the National Security Agency's domestic surveillance program broke in December, the debate—a heated one—was about whether the president, by authorizing it, had broken the law. Along with Democrats, some Republicans in the House and Senate expressed doubts about the program’s legality. Despite Senate committee hearings and a White House publicity campaign, that question is hardly resolved.

This week, however, congressional Republicans pushed the debate in a new direction. Even as they prepare to investigate some aspects of the NSA program, many are apparently willing to accept that warrantless surveillance of Americans is an important tool in tracking terrorists. Some members of Congress are now asking how they can revise the law to make domestic eavesdropping legal some of the time.

The law in question, the Foreign Intelligence Surveillance Act, or FISA, which has governed domestic surveillance since 1978, requires the government to apply to a special court for a warrant in order to conduct surveillance for intelligence purposes on US soil. In a warrant application, investigators must show they have probable cause to believe that their target is a foreign power or its agent. The NSA program approved by President Bush did not go through the FISA court—instead, the agency has been tapping the phones and reading the e-mail of US residents without warrants.

Scraping court-approved warrants for some category of domestic wiretaps would be a major departure for American law. So while congressional Republicans are beginning to argue, along with the president, that such a step is necessary because of the value of the NSA program to national security, Democrats (and many scholars) think it’s entirely premature. They want to keep the focus on whether Bush exceeded his authority in
approving the program in the first place. For better or worse, however, efforts to find a legal framework to accommodate warrantless wiretapping are already underway. The tug of war over what could be one of the most important changes to American law in a generation reveals very different opinions about how best to balance national security and civil liberties—and who should watch the watchers.

Of course, any public discussion about the legality of warrantless wiretapping must take place, to some extent, in ignorance. Exactly who is being selected for surveillance, or how, or how often the eavesdropping yields valuable intelligence remains classified. Does every NSA wiretap meet the legal standard of probable cause, as Attorney General Alberto Gonzales has repeatedly said? Or does the program also include fishing expeditions, in which investigators aren't listening in on targets but rather mining data to figure out who to target, as has been widely reported? Is it a tool that's making the NSA considerably better at finding terrorists, or one that sells out civil liberties on the cheap?

Senator Mike DeWine, an Ohio Republican, is ready to give the president and the NSA the benefit of the doubt. He is drafting legislation that "would exempt the terrorism surveillance program from the FISA statute," according to spokesman Mike Dawson. Under DeWine's proposed law, the NSA would still have to show probable cause to obtain a warrant for a wiretap, but the warrant application wouldn't be reviewed by the FISA court. Instead, two congressional committees, one in the House and one in the Senate—each composed of three Democrats and three Republicans—would, in Dawson's words, "exercise oversight" in the way that congressional committees always do over intelligence matters. But Dawson made clear this would not mean members of Congress would scrutinize each warrant application to make sure the facts supporting it amount to probable cause.

It's unclear, then, what such oversight would amount to—a question mark that's sure to alarm civil libertarians even as it pleases the president. The White House indicated its support for the proposal on Wednesday in a call from White House counsel Harriet Miers to DeWine's office.

Federal Appeals Court Judge Richard Posner has a different proposal—one that would jettison warrants and probable cause altogether. In a Wall Street Journal op-ed piece this week, Posner called FISA "dangerously obsolete" and "hopeless as a framework for detecting terrorists." Warrants obtained with probable cause, he argues, are the right tool when the government knows who its target is but fail when you're trying to figure out who to target in the first place.

Posner would place oversight of the NSA program in the hands of a "steering committee" composed of the attorney general, the director of national intelligence, the secretary of homeland security, and a senior or retired federal judge to be appointed by the chief justice of the Supreme Court. In other words, oversight of the executive branch would be controlled by the executive branch—also setting off civil liberties alarms.

It's not clear whether DeWine's and Posner's proposals would pass constitutional muster. Traditionally, Fourth Amendment law gives the judiciary, not the legislature or the executive, the role of ensuring that the government doesn't intrude on individual privacy through unreasonable searches and seizures. Decisions made by legislators and the president are inherently political. Life-tenured judges are better positioned to stand up for individual rights, however unpopular or inexpedient it may be to do so.

Philip Heymann, a professor at Harvard Law School, debated Posner about the merits and legality of the NSA program on The New Republic's website last week. He doesn't think the changes proposed by DeWine and Posner are necessary. "We shouldn't consider rewriting FISA unless someone can convince us that whatever powers are granted will really help significantly in preventing terrorism," he says.

But if he were to be convinced that FISA needed amending, Heymann says, he'd start with more incremental change that would leave the Fourth Amendment's guarantees undisturbed. Consider, for example, the difference between what you write on the outside of an envelope—the name and address of the recipient, and your own—and the
letter you put inside.

The law already makes a distinction between content—what we say on a phone call or in an e-mail—and "routing and addressing information"—the phone numbers and e-mail addresses of people we communicate with. Content normally gets lots of constitutional protection. Routing information, on the other hand, does not—you don't see detectives on "Law & Order" waiting around for a judge before they pull a perp's phone records. That's because in a 1979 case, Smith v. Maryland, the Supreme Court ruled that type of information merits no Fourth Amendment protection.

If the government wants to review massive amounts of routing information—for example by tapping a fiber-optic cable that carries a billion messages a day—such trawling would be perfectly constitutional. As currently written, however, FISA isn't exactly set up to allow for such broad collection of information. The statute, enacted long before the days of e-mail, anticipates that the government will identify a particular target when it applies for a warrant from the FISA court, and certify that the wiretap is relevant to an intelligence investigation. If Congress eliminated the certification requirement, Heymann says, "I don't think anyone would lose any privacy."

Heymann can also imagine giving the government freer rein to use a Google-like search engine to look for key words or phrases in the content of massive amounts of domestic calls and e-mails, as long as the NSA isn't targeting particular individuals. "That would be far less important in terms of civil liberties than tapping and listening to all my conversations," he says.

But if civil libertarians are willing to give ground in some ways, they're still adamant about resolving the question of whether the president had the power to approve the NSA program on his own. And they want the courts to be the branch to do it. Harvard law professor David Barron proposes amending FISA so that Americans who can show that their ability to speak freely on the phone or in e-mails has been abridged for fear the NSA may be listening—because they frequently call a mosque in Afghanistan, for example—can go to court to argue that their rights have been violated.

"The way this should be resolved eventually is by the courts," Barron said. "It's obvious why the administration doesn't want that, because it's the one forum in which it's really afraid it will lose."

Lawsuits challenging domestic eavesdropping have already been brought, but their trajectory is uncertain. Since the journalists and other plaintiffs bringing suit don't know for sure they've been spied on, they may have trouble getting into court unless Congress makes clear they have a right to.

Emily Bazelon is a senior editor at Slate.

© Copyright 2006 Globe Newspaper Company.