U.S. Pushes to Ease Technical Obstacles to Wiretapping

By CHARLIE SAVAGE
Published: October 18, 2010

WASHINGTON — 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, federal officials say.

The officials say tougher legislation is needed because some telecommunications companies in recent years have begun new services and made system upgrades that create technical obstacles to 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 a 1994 law requiring carriers to make sure their systems can be wiretapped. There is not yet agreement over the details, according to officials familiar with the deliberations, but they said the administration intends to submit a package to Congress next year.

To bolster their case, security agencies are citing two previously undisclosed episodes in which major carriers were stymied for weeks or even months when they tried to comply with court-approved wiretap orders in criminal or terrorism investigations, the officials said.

Albert Gidari Jr., a lawyer who represents telecommunications firms, said corporations were likely to object to increased government intervention in the design or launch of services. Such a change, he said, could have major repercussions for industry innovation, costs and competitiveness.

“The government’s answer is ‘don’t deploy the new services — wait until the government
catches up," Mr. Gidari said. "But that’s not how it works. Too many services develop too quickly, and there are just too many players in this now."

Under the 1994 law, the Communications Assistance to Law Enforcement Act, telephone and broadband companies are supposed to design their services so that they can begin conducting surveillance of a target immediately after being presented with a court order.

Officials from the Justice Department, the National Security Agency, the F.B.I. and other agencies recently began working on a draft of a proposal to strengthen and expand that law. There is not yet internal agreement over its details, according to officials familiar with the deliberations, but they said the Obama administration intended to submit a package to Congress next year.

The disclosure that the administration is seeking ways to increase pressure on carriers already subject to the 1994 law comes less than a month after The New York Times reported on a related 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.

The push to expand 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 also be used by repressive regimes to hunt for political dissidents.

An F.B.I. spokesman said the bureau would not comment about the telecom proposal, citing the sensitivity of internal deliberations. But last month, in response to questions about the Internet communications services proposal, Valerie E. Caproni, the F.B.I.’s general counsel, emphasized that the government was seeking only to prevent its surveillance power from eroding.

Starting in late 2008 and lasting into 2009, another law enforcement official said, a “major” communications carrier was unable to carry out more than 100 court wiretap orders. The initial interruptions lasted eight months, the official said, and a second lapse lasted nine days.

This year, another major carrier experienced interruptions ranging from nine days to six weeks and was unable to comply with 14 wiretap orders. Its interception system “works sporadically and typically fails when the carrier makes any upgrade to its network,” the official said.

In both cases, the F.B.I. sent engineers to help the companies fix the problems. The bureau spends about $20 million a year on such efforts.

The official declined to name the companies, saying it would be unwise to advertise which networks have problems or to risk damaging the cooperative relationships the government has with them. For similar reasons, the government has not sought to penalize carriers over wiretapping problems.

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.

Once a carrier’s interception capability is restored — even if it is at taxpayer expense — its service is compliant again with the 1994 law, so the issue is moot.

The F.C.C. also moves slowly, officials complain, in handling disputes over the “safe harbor” standard. For example, in 2007 the F.B.I. asked for more than a dozen changes, like adding a mandate to turn over more details about cellphone locations. The F.C.C. has still not acted on that petition.

Civil liberties groups contend that the agency has been far too willing on other occasions to expand the reach of the 1994 law.

“We think that the F.C.C. has already conceded too much to the bureau,” said Marc Rotenberg, the president of the Electronic Privacy Information Center. “The F.B.I.’s ability to have such broad reach over technical standard-setting was never anticipated in the 1994 act.”

The Obama administration is circulating several ideas for legislation that would increase the government’s leverage over carriers, officials familiar with the deliberations say.

One proposal is to increase the likelihood that a firm pays a financial penalty over wiretapping lapses — like imposing retroactive fines after problems are fixed, or billing companies for the cost of government technicians that were brought in to help.

Another proposal would create an incentive for companies to show new systems to the F.B.I. before deployment. Under the plan, an agreement with the bureau certifying that the system is acceptable would be an alternative “safe harbor,” ensuring the firm could not be fined.
Bloggingheads: Christians and Gay Suicide
Is Christian fundamentalism to blame for antigay bullying?