GlobalResearch
Center for Research on Globalization

U.S. Wants to Make It Easier to Wiretap the Internet

By Charlie Savage

Theme: Police State & Civil Rights

Global Research, September 27, 2010
New York Times 27 September 2010

WASHINGTON — Federal law enforcement and national security officials are preparing 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.

The bill, which the Obama administration plans to submit to lawmakers next year, raises fresh questions about how to balance security needs with protecting privacy and fostering innovation. And because security services around the world face the same problem, it could set an example that is copied globally.

James X. Dempsey, vice president of the Center for Democracy and Technology, an Internet policy group, said the proposal had “huge implications” and challenged “fundamental elements of the Internet revolution” — including its decentralized design.

“They are really asking for the authority to redesign services that take advantage of the unique, and now pervasive, architecture of the Internet,” he said. “They basically want to turn back the clock and make Internet services function the way that the telephone system used to function.”

But law enforcement officials contend that imposing such a mandate is reasonable and necessary to prevent the erosion of their investigative powers.

“We’re talking about lawfully authorized intercepts,” said Valerie E. Caproni, general counsel for the Federal Bureau of Investigation. “We’re not talking expanding authority. We’re talking about preserving our ability to execute our existing authority in order to protect the public safety and national security.”

Investigators have been concerned for years that changing communications technology could damage their ability to conduct surveillance. In recent months, officials from the F.B.I., the Justice Department, the National Security Agency, the White House and other agencies have been meeting to develop a proposed solution.

There is not yet agreement on important elements, like how to word statutory language defining who counts as a communications service provider, according to several officials familiar with the deliberations.

But they want it to apply broadly, including to companies that operate from servers abroad, like Research in Motion, the Canadian maker of BlackBerry devices. In recent months, that company has come into conflict with the governments of Dubai and India over their inability to conduct surveillance of messages sent via its encrypted service.

In the United States, phone and broadband networks are already required to have interception capabilities, under a 1994 law called the Communications Assistance to Law Enforcement Act. It aimed to ensure that government surveillance abilities would remain intact during the evolution from a copper-wire phone system to digital networks and cellphones.

Often, investigators can intercept communications at a switch operated by the network company. But sometimes — like when the target uses a service that encrypts messages between his computer and its servers — they must instead serve the order on a service provider to get unscrambled versions.

Like phone companies, communication service providers are subject to wiretap orders. But the 1994 law does not apply to them. While some maintain interception capacities, others wait until they are served with orders to try to develop them.

The F.B.I.'s operational technologies division spent $9.75 million last year helping communication companies — including some subject to the 1994 law that had difficulties — do so. And its 2010 budget included $9 million for a "Going Dark Program" to bolster its electronic surveillance capabilities.

Beyond such costs, Ms. Caproni said, F.B.I. efforts to help retrofit services have a major shortcoming: the process can delay their ability to wiretap a suspect for months.

Moreover, some services encrypt messages between users, so that even the provider cannot unscramble them.

There is no public data about how often court-approved surveillance is frustrated because of a service's technical design.

But as an example, one official said, an investigation into a drug cartel earlier this year was stymied because smugglers used peer-to-peer software, which is difficult to intercept because it is not routed through a central hub. Agents eventually installed surveillance equipment in a suspect's office, but that tactic was "risky," the official said, and the delay "prevented the interception of pertinent communications."

Moreover, according to several other officials, after the failed Times Square bombing in May, investigators discovered that the suspect, Faisal Shahzad, had been communicating with a service that lacked prebuilt interception capacity. If he had aroused suspicion beforehand, there would have been a delay before he could have been wiretapped.

To counter such problems, officials are coalescing around several of the proposal's likely requirements:

¶ Communications services that encrypt messages must have a way to unscramble them.

¶ Foreign-based providers that do business inside the United States must install a domestic

office capable of performing intercepts.

¶ Developers of software that enables peer-to-peer communication must redesign their service to allow interception.

Providers that failed to comply would face fines or some other penalty. But the proposal is likely to direct companies to come up with their own way to meet the mandates. Writing any statute in "technologically neutral" terms would also help prevent it from becoming obsolete, officials said.

Even with such a law, some gaps could remain. It is not clear how it could compel compliance by overseas services that do no domestic business, or from a "freeware" application developed by volunteers.

In their battle with Research in Motion, countries like Dubai have sought leverage by threatening to block BlackBerry data from their networks. But Ms. Caproni said the F.B.I. did not support filtering the Internet in the United States.

Still, even a proposal that consists only of a legal mandate is likely to be controversial, said Michael A. Sussmann, a former Justice Department lawyer who advises communications providers.

"It would be an enormous change for newly covered companies," he said. "Implementation would be a huge technology and security headache, and the investigative burden and costs will shift to providers."

Several privacy and technology advocates argued that requiring interception capabilities would create holes that would inevitably be exploited by hackers.

Steven M. Bellovin, a Columbia University computer science professor, pointed to an episode in Greece: In 2005, it was discovered that hackers had taken advantage of a legally mandated wiretap function to spy on top officials' phones, including the prime minister's.

"I think it's a disaster waiting to happen," he said. "If they start building in all these back doors, they will be exploited."

Susan Landau, a Radcliffe Institute of Advanced Study fellow and former Sun Microsystems engineer, argued that the proposal would raise costly impediments to innovation by small startups.

"Every engineer who is developing the wiretap system is an engineer who is not building in greater security, more features, or getting the product out faster," she said.

Moreover, providers of services featuring user-to-user encryption are likely to object to watering it down. Similarly, in the late 1990s, encryption makers fought off a proposal to require them to include a back door enabling wiretapping, arguing it would cripple their products in the global market.

But law enforcement officials rejected such arguments. They said including an interception capability from the start was less likely to inadvertently create security holes than retrofitting it after receiving a wiretap order.

They also noted that critics predicted that the 1994 law would impede cellphone innovation, but that technology continued to improve. And their envisioned decryption mandate is modest, they contended, because service providers — not the government — would hold the key.

“No one should be promising their customers that they will thumb their nose at a U.S. court order,” Ms. Caproni said. “They can promise strong encryption. They just need to figure out how they can provide us plain text.”

Articles by: Charlie Savage