TechNewsDaily™
Where technology meets daily life.

New Surveillance Laws Could Cripple Facebook, Google, US Innovation

By: Paul Wagenseil – May 1, 2013

New legislation would slap monetary penalties on Facebook, Google and other Internet companies for resisting law-enforcement surveillance requests, according to a new report.

Unnamed sources told the Washington Postin a story published Sunday (April 28) that a government task force was preparing amendments to the 1994 Communications Assistance for Law Enforcement Act (CALEA) and the 1968 Wiretap Act.

The new laws would force online service providers to build in deliberate software flaws to let law enforcement listen in on consumer-grade encrypted communications — or face fines for not cooperating.

The list of American software companies that could be affected is a Who's Who of the Internet: AOL, Apple, Facebook (which also owns Instagram), Google, Microsoft, SnapChat, WhatsApp and Yahoo.

Yet a prominent critic says the new laws wouldn't work, and would in fact cripple American companies' ability to innovate against foreign competition.

"This is an insanely bad idea on a number of levels," Julian Sanchez, a research fellow at the libertarian Cato Institute in Washington, D.C., told TechNewsDaily.

"It's not really going to be much use against the most serious and sophisticated criminals," Sanchez said. "If you announce that all U.S. companies are going to have mandatory law-enforcement backdoors, they'll either use secure foreign services or implement their own client-side encryption."

Facebook and Google did not immediately respond to requests for comment. [10 Ways the Government Watches You]

Resistance is futile

Both CALEA and the Wiretap Act established rules by which law enforcement can eavesdrop on U.S. and foreign residents. Neither outlines what governments can do in case the owners of the means of communications don't comply.

Google has developed a reputation for resisting government requests. In 2006, the company went to court rather than submit to a warrant seeking the search records of suspected child pornographers.

Last year, it forced the FBI to get a warrant to "unlock" a suspected pimp's Android phone, then refused to hand over the requested information once the warrant was provided.

Google also publicly discloses how many requests it gets from law enforcement for information about clients.

According to the Post report, the proposed legislation would extend CALEA, which now clearly applies only to telecommunications, networking and Voice over Internet Protocol providers, to definitively cover makers of Internet communications software.

But the meat of the law would add some teeth to the Wiretap Act. It would allow a court to levy fines on firms that don't comply with eavedropping orders. After 90 days of noncompliance, the fines would double daily.

To Sanchez, the amendments would stifle innovation and make American companies less competitive.

"You're telling thousands upon thousands of companies, many of which are constantly redesigning and rolling out new services, that they've all got to factor this capability in from the outset whenever they develop new functionality," he said.

"It's fundamentally contrary to the spirit of the 'end to end' principle of permissionless innovation that has made the Internet such an incredible engine of both economic and cultural growth."

Flipping the switch

CALEA compliance is generally built into modern telephone, broadband and networking equipment. If presented with a warrant, the company concerned can just flip a switch to let law enforcement listen in.

But the rapid growth of end-to-end-encrypted services that traverse the Internet have left CALEA in the dust, and law enforcement in the dark.

Several FBI officials have warned of the "going dark" problem, in which terrorists, drug dealers and child pornographers will be able to use encrypted services like BlackBerry Messenger or Apple's iMessage without fear of the fuzz listening in.

"It is critically important that we have the ability to intercept electronic communications with court approval," former FBI General Counsel Valerie Caproni told a House subcommittee in February 2011. "We confront, with increasing frequency, service providers who do not fully comply with court orders in a timely and efficient manner."

"Those communications are being used for criminal conversations," Andrew Weissmann, Caproni's successor as FBI general counsel, told the American Bar Association last month.

Security experts have already warned that building "backdoors" into communication software would open the door to hackers.

Sanchez agrees with that assessment, and downplays the importance of the ability to wiretap.

"To say that communications have to be accessible to law enforcement means, effectively, that companies have to build a security vulnerability into their systems," he said. "It's like requiring every lock to be capable of opening with the same master key just in case the cops want to search your home."