Push for US Internet 'wiretap' law faces tough road

June 2 2013, by Rob Lever

The FBI is stepping up its effort to get broader authority to put "wiretaps" on the Internet to catch criminals and terrorists. But the move is drawing fire from civil liberties groups, technology firms and others who claim the effort could be counterproductive, by harming online security and imposing hefty costs on makers of hardware and software.

US law enforcement has for years complained about the problem of "going dark," or being unable to monitor Internet communications in the same manner as wiretaps, for which officials get a court order to tap into a local phone company.

President Barack Obama said in a May 23 speech his administration is "reviewing the authorities of law enforcement, so we can intercept new types of communication."

FBI general counsel Andrew Weissmann told a recent Washington forum it would be "a top priority this year" to get expanded authority to tap communications such as "Gmail, Google voice (and) Dropbox."

"The way we communicate today is not limited to telephone companies," Weissmann said. "What we don't have is the ability to go to court and require the recipient to effectuate the intercept. Most countries have that."

The FBI can get a court order to monitor Internet-based communications under current law, and major companies like Google and Microsoft may

be able to comply.

But many other firms lack the technical capacity to allow this kind of surveillance. The proposal under consideration, according to published reports, would require firms to enable government access or face hefty fines.

The US administration has made no public proposal on wiretap authority, but even the hint of a change has sparked a heated response.

Critics say such a move would be tantamount to giving the government a "backdoor" to every piece of hardware and software being used, which could be exploited by hackers, foreign governments or others.

"It's an intentional security vulnerability that they hope will only be used by the good guys, but we have evidence that the bad guys use it too," said Joseph Hall, senior technologist at the Center for Democracy and Technology, a digital rights organization.

Hall said that to make the program work, law enforcement would need to get "all the encryption keys" for hardware and require software to be designed with so-called backdoor access, imposing new costs on technology firms.

A CDT report endorsed by 20 security and technology experts underscored the problems with any new Internet surveillance authority.

Mandating a virtual wiretap "is harmful," said Edward Felten, a Princeton University computer scientist who was among those endorsing the report.

"The port makes it easier for attackers to capture the very same data that law enforcement wants," he said in a blog posting.

"Better yet (for the intruder), the capability will be stealthy by design, making it difficult for the user to tell that anything is amiss," he added.

"Beyond this, the mandate would make it harder for users to understand, monitor, and fix their own systems—which is bad for security."

Bruce Schneier, a computer security and cryptography expert, said the proposal would be "horribly ineffective."

"Mandating wiretap capability in vast swaths of software will render normal law-abiding people less secure, while allowing criminals and terrorists to disable the wiretap capability or use more secure products from other countries," he said.

Technology companies also fiercely oppose any measure leading to government access, saying it would stifle innovation, impose costs on US firms and make their products less competitive in global markets.

"The Department of Justice has not made the case for granting law enforcement broad new powers over Internet companies for purposes of new wiretap authority," said Michael Beckerman of the Internet Association, a lobby for tech companies.

"There are a number of serious unintended consequences with this flawed proposal. A wiretap mandate for the Internet is dead on arrival."

CDT's Hall said recent investigations suggest the FBI and other law enforcement agencies already collect vast amounts of information that could help prevent crimes but fail to make use of it.

"Maybe it's time to use the mountains of information the FBI collects in a smarter way rather than trying to get more information," he said.