THE HILL

Silicon Valley spars with Obama over 'backdoor' surveillance

By Cory Bennett - 03/22/15 09:00 AM EDT

Silicon Valley and a bipartisan group of lawmakers are lining up against the Obama administration, criticizing what they see as a lack of support for total online privacy.

The steady rise of sophisticated privacy techniques such as encryption and anonymity software has put the government in a difficult position — trying to support the right to privacy while figuring out how to prevent people from evading law enforcement.

“The technologies are evolving in ways that potentially make this trickier,” President Obama said during a January news conference with British Prime Minister David Cameron.

The conundrum has led to a heated debate in Washington: Should law enforcement have guaranteed access to data?

“I think there’s a little bit of a tug of war happening in the government,” said Jay Kaplan, co-founder of the security firm Synack and a former National Security Agency (NSA) cyber analyst.

The Obama administration — from officials with FBI and the National Security Agency (NSA) to the president himself — has come out in favor of some form of guaranteed access while still endorsing strong encryption.

“If we get into a situation in which the technologies do not allow us at all to track somebody that we're confident is a terrorist,” Obama said, “that's a problem.”

What shape that access takes, however, is unclear.

“The dialogue that we're engaged in is designed to make sure that all of us feel confident that if there is an actual threat out there, our law enforcement and our intelligence officers can identify that threat and track that threat at the same time that our governments are not going around phishing into whatever text you might be sending on your smartphone,” Obama said. “And I think that's something that can be achieved.”

Privacy hawks on Capitol Hill aren’t buying it.

“I don’t think much of that,” Rep. Joe Barton (R-Texas), co-founder of the Congressional Bipartisan Privacy Caucus, told The Hill. “We have a huge homeland security apparatus with almost unlimited authority to — with some sort of a reasonable suspicion — check almost any type of communication, whether it’s voice, Internet, telephonic, electronic, you name it.”

“Those were positions that did not receive rave reviews here in Silicon Valley,” said Rep. Zoe Lofgren (D-Calif.), whose district includes parts of tech-heavy San Jose.

Many believe the administration’s stance is inherently at odds with robust digital protection.

“In order to fully implement what he's suggesting, you would need one of two things,” Lofgren said.

One would be installing so-called “backdoors” in encryption — an access point known only to law enforcement agencies. Security experts find this concept abhorrent, since cyber crooks or foreign intelligence agencies would likely exploit it.

“There’s no safe way to do that,” Kaplan said. “It’s just an impossible task. Just a bad idea all together.”

The second would be to have a third-party company hold all user data, with some sort of agreement to disclose information to the government, Lofgren said.

“I think actually the trend line is in a different direction, which is encryption that is not accessible to the companies that provide it, either,” she added.

Major tech companies like Apple have done exactly that, claiming that even they can’t unlock data on newer devices.

“In many cases the actions of government, or the interests of government, may be juxtaposed to private enterprises, and that’s the way the world works,” said Kevin Bocek, vice president of security strategy and threat intelligence at Venafi. “We’ve got a democracy and that’s going to be played out.”

Lofgren, along with Reps. Thomas Massie (R-Ky.) and Jim Sensenbrenner (R-Wis.), introduced in December the Secure Data Act, which would ban the government from compelling tech companies to create backdoor vulnerabilities.

NSA critic Sen. Ron Wyden (D-Ore.) has backed a Senate version of the bill.

Lofgren hopes the measure will ensure encryption is part of the debate when the NSA’s key surveillance programs are up for reauthorization this summer.

“That doesn’t mean it will in fact be part of the final bill,” Lofgren said. “I don’t think it’s something the Republican leadership has embraced so far.”

“But I do think that right now the status quo protects the right of companies to encrypt,” she added. “I think that’s a status quo likely to go on for awhile.”

Administration officials defend what they see as a strong record of supporting the right to encrypt.

Just last week, White House Cybersecurity Coordinator Michael Daniel insisted that “[Obama] actually said there is no scenario in which the U.S. government does not support strong encryption.”

Security experts do give the administration credit for going to great lengths to strengthen digital privacy in some areas.

The U.S. government provides roughly 75 percent of the funds used to run Tor, the world’s leading online anonymity software, said Andrew Lewman, executive director of the Tor Project.

“The people who fund us really like Tor,” Lewman said. “We’re totally happy there.”

The technology is a main tool helping Chinese citizens evade the country’s growing Internet censorship efforts. *The New York Times* and *The New Yorker* have used the software to create anonymous drop boxes for whistleblowers. Tor’s open source code is being used to generate dozens of other online anonymity products.

The software has grown steadily in recent years and has reached 2.5 million daily users, Lewman said. It’s now the global standard bearer.

Synack’s Kaplan also thinks government officials are coming around to the idea that backdoors are not feasible, that they can’t have “both sides of the coin.”

“If you’re going to create very safe encryption standards that work unilaterally across all communications, then you're going to inherently have problems in certain aspects,” Kaplan said.

House Intelligence Committee Chairman Devin Nunes (R-Calif.) recognizes the need to work with private industry and security officials on “devising a path forward on encryption,” he told The Hill via email. “The goal is to protect individuals’ privacy while ensuring that law enforcement officials are not prevented from tracking criminals and terrorists.”

It’s not a goal easily achieved.

“How do you ultimately strike the right balance?” Kaplan said. “I think that’s just a fundamental question the government will continue to grapple with.”

The Hill 1625 K Street, NW Suite 900 Washington DC 20006 | 202-628-8500 tel | 202-628-8503 fax