WINSTON-SALEM JOURNAL

Data encryption bill sponsored by Burr, Feinstein meets resistance

Bertrand M. Gutiérrez

April 17, 2016

The fate of a draft bill announced last week by U.S. Sens. Richard Burr, R-N.C., and Dianne Feinstein, D-Calif., remains uncertain as members of Congress and the private sector say its attempt to deal with encryption technology, national security concerns and the privacy rights of consumers is severely flawed.

The bill would affect people and businesses that traffic in data: programmers, app developers and service providers such as YouTube or device-makers such as Apple, among other entities, according to Julian Sanchez, a senior fellow at the Cato Institute, a libertarian research group based in Washington.

They would be obligated to make sure that evidence obtained by the government is readable. They would have to decrypt data that is encrypted by their software or provide the technical assistance to do so, Sanchez said.

“From Google to the teen writing an app in his basement, this would apply to them,” he said.

“Every technology company expert I’ve seen who has had a reaction to this bill has been appalled, and it’s not because they’re hippies,” Sanchez said, later adding, “It’s like saying all you have to do is build a perpetual-motion machine.”

Encryption is routine

Encryption technology is part of everyday life on the Internet. When it works, it blocks hackers from seeing private communications between Internet users and their banks, for example.

The technology can also block law enforcement agencies.

That’s why the FBI sought a court order forcing Apple to help the bureau access the iPhone used by one of the shooters in the attack in San Bernardino, Calif.

Apple Chief Executive Tim Cook resisted, backed by other technology company representatives, saying the government should not force the company to create software to hack into its own device. In the end, the FBI found a way to hack into the phone without Apple's help.

Had the Burr-Feinstein bill been in effect, Apple would have been required to decrypt the data.

Challenger's response

Burr's Democratic challenger in this November's Senate race, Deborah Ross, was asked where she stands on the bill.

"I strongly believe that we can keep our citizens safe while also protecting the privacy rights of law-abiding Americans," Ross said. "To do that, our legislative efforts need to be precise, so that we are not putting people's personal information at risk unnecessarily or making our country more vulnerable to attack.

"No company is above the law," she said, echoing the introduction to the bill: "It is the sense of Congress that no person or entity is above the law."

Efforts to contact Libertarian U.S. Senate candidate Sean Haugh were unsuccessful.

Republican and Democratic members of Congress lambasted the bill, saying the proposal would weaken encryption technology that is designed to shield Internet users from hackers.

U.S. Sen. Ron Wyden, D-Ore., said he would block the bill with a filibuster if it reaches the Senate floor.

"This flawed bill would leave Americans more vulnerable to stalkers, identity thieves, foreign hackers and criminals," said Wyden, a member of the Senate Select Committee on Intelligence.

"And yet it will not make us safer from terrorists or other threats. Bad actors will continue to have access to encryption, from hundreds of sources overseas," he said.

Wyden, Feinstein and Burr are members of the Senate Select Committee on Intelligence. Burr is the committee chairman, and Feinstein is the vice chairwoman.

U.S. Rep. Darrell Issa, R-Calif., said the bill is as "technically naive as a piece of legislation can get."

"Mandating that companies weaken our security to give government secret backdoor access into our devices would be a massive blow to American's right to privacy and frankly would also be downright dangerous," said Issa, the chairman of the House judiciary subcommittee that deals with Internet policy.

Antiquated laws

The proposal would affect such businesses as device manufacturers, software manufacturers, and communications services, according to Burr's aides.

"Covered entities that receive a court order for information or data for the investigation or prosecution of specified serious crimes must provide it to the government in an intelligible

format or provide the technical assistance necessary to do so," Burr's aides said in a description of the draft bill.

For his part, Burr told the Winston-Salem Journal in February that the growing divide between antiquated laws and emerging encryption technologies merits more debate.

"I have long believed that data is too insecure and feel strongly that consumers have a right to seek solutions that protect their information — which involves strong encryption," Burr said last week. "I do not believe, however, that those solutions should be above the law.

Mitch Kokai, a senior policy analyst at the conservative John Locke Foundation, based in Raleigh, said Burr and Feinstein are wise to encourage more discussion.

"National security and individual privacy are both highly important to our society," Kokai said.

"We should not want to open the door too widely for government to snoop into our activities.

"Nor should we want privacy concerns to trump security interests when there's a compelling case that encrypted information can help prevent a terrorist plot," he said.