Senators clash over WhatsApp’s encryption update

thehill.com/policy/cybersecurity/275393-senators-clash-over-whatsapps-encryption-update

4/6/2016

By Cory Bennett - 04/06/16 04:28 PM EDT

Two lawmakers issued dueling statements on Wednesday alternately praising and bashing the popular messaging platform WhatsApp for turning on default encryption for its billion users.

“This is especially important for human rights activists, political dissidents and persecuted minorities around the world,” said Sen. Ron Wyden (D-Ore.).

“This is an open invitation to terrorists, drug dealers and sexual predators to use WhatsApp’s services to endanger the American people,” countered Sen. Tom Cotton (R-Ark.).

The remarks came a day after Facebook-owned WhatsApp said it had extended automatic end-to-end encryption to all of its users, meaning only the sender and recipient of a message can view its content.

The move strengthens privacy for WhatsApp users but also potentially locks out law enforcement officials who want to use the communications in an investigation.

The lawmakers' opposing reactions reflect the divisive rhetoric of the encryption debate on Capitol Hill since the terror attacks in Paris; San Bernardino, Calif., and Brussels.

Some members, such as Cotton, say the events highlight the need to give law enforcement greater power to decipher encrypted data. WhatsApp's move only makes the need more urgent, he argued.

“I strongly urge WhatsApp and Facebook to reevaluate their decision before they help facilitate another terrorist attack,” Cotton said Wednesday.

But others, like Wyden, say guaranteeing government access to secure platforms weakens global security for all.

“While some continue to spread fear about modern technology, the fact is strong encryption is essential to

Americans' individual security," the Oregon Democrat said.

The decision to make end-to-end encryption the default for all WhatsApp users is just the latest push from prominent tech companies to expand encryption across their services and devices.

The trend has created considerable friction between the tech community and law enforcement agencies.

These tensions recently spilled over in a court battle between Apple and the FBI over a locked iPhone used by one of the shooters in the San Bernardino, Calif., terror attack.

The FBI claimed Apple's security measures, including strong encryption, had made it impossible to access the phone without the company's help. The bureau got a court order directing the company to create software that would allow investigators to hack into the phone.

But Apple rebuffed the request, arguing that complying would create a "backdoor" into all iPhones and set a troubling precedent empowering the government to force companies to decrypt data upon request.

The FBI ultimately cracked the phone through another method and dropped its case.

Cotton chastised WhatsApp for following in Apple's footsteps, calling it part of a "dangerous trend."

"We cannot allow companies to purposefully design applications that make it impossible to comply with court orders," he said.

Sens. Richard Burr (R-N.C.) and Dianne Feinstein (D-Calif.) — the leaders of the Senate Intelligence Committee — are expected to soon release a bill that would force tech companies to comply with such court orders seeking locked data.

But Wyden countered that these lawmakers are being unrealistic. Even if WhatsApp didn't offer end-to-end encryption, popular chatting platforms in other countries would, Wyden explained.

"While law enforcement agencies have legitimate concerns about challenges caused by encryption, the solution is to adapt, by developing new techniques and resources for the digital age," he said.

"Attacking the use of strong encryption only empowers criminals, foreign hackers and predators who will take advantage of weak digital security."