Business

Debate over encryption 'backdoors' escalates

By Andrea Peterson
The Washington Post

JANUARY 11, 2016, 1:27 PM

Nearly 200 experts, companies and civil society groups from more than 40 countries are asking governments around the world to support strong encryption — and reject proposals that would undermine the digital security it provides.

"The internet belongs to the world's people, not its governments. We refuse to let this precious resource become nationalized and broken by any nation," Brett Solomon, executive director of Access Now, the online advocacy group that organized the open letter, said in a news release.

The letter, released online in 10 languages Monday at SecureTheInternet.org, marks an escalation of a debate over encryption — a process that scrambles data so that only those authorized can decode it. The fight has been brewing in the United States for more than a year, but has also spread everywhere from the United Kingdom to China.

Encryption is widely relied on to keep e-commerce and many of the websites people use every day safe from the prying eyes of cybercriminals. But the spread of the strongest forms of encryption, those which companies themselves cannot unlock, into products from major tech companies has drawn the criticism from some law enforcement officials who argue that it may allow criminals and terrorists to "go dark."

Tech companies, the officials have argued, should make sure that they are able to provide access to encrypted content for law enforcement when faced with a court order. However, technical experts say building ways for that access into products — commonly called a "backdoor" — would undermine digital security as a whole by giving hackers a new target. And civil liberties experts worry that there's nothing to stop repressive governments from pushing for the same access.

"Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age," said David Kaye, a law professor at the University of California Irvine and

United Nations Special Rapporteur for Freedom of Opinion and Expression, who released a report on the issue last year.

The U.S. debate seemed all but over in October, when the Obama administration said it had decided against pushing for legislation mandating backdoors, at least for the time being. But the issue gained new steam in light of attacks by terrorists in California and Paris last fall, which some reports linked to encrypted communications.

Last Friday, White House officials met with the leaders of major tech companies about how they could help combat the Islamic State. Encryption was on the agenda, although it seems unlikely that tech companies would change position on the issue. Trade groups representing major tech companies including Microsoft, Facebook and Google signed onto the Monday letter.

Access Now began organizing for the letter this fall after putting together a White House petition asking the Obama administration to come out against encryption backdoors. The administration requested further pubic input and sat down with Access Now and other advocates last month, but it has not yet released a final response.

The White House declined to comment on the letter or the status of its response to the earlier petition. The president has previously stated his support for "strong encryption," but it's unclear whether the administration's definition of the term lines up with that of civil liberties advocates.

But the administration's stance isn't just a domestic issue, advocates argue. "That lack of leadership is reverberating around the world," said Nathan White, senior legislative manager at Access Now.

Many countries are considering — or have even already passed — legislation that experts say could undermine the protection provided by encryption, and civil society groups are spread thin trying to fight them, he said.

The United Kingdom is considering a proposal that would require tech companies to build ways to intercept encrypted communications into their products. The plan has drawn formal complaints from tech companies including Apple, Google, Facebook, Microsoft, Twitter and Yahoo. And in December, China passed an anti-terrorism law that requires companies to provide "technical interfaces" and assist with decryption if the country's security forces say it's necessary.

But thanks to the global nature of the Internet, advocates argue that such national laws can have global implications because it leaves tech companies with a only a few options: Pull out of the country, provide a less-secure version of their services to users there, or roll out a less secure version around the world.

"A threat anywhere is devastating everywhere," White said.

The Washington Post