Could Twitter stop the next terrorist attack?

July 24 2015, byAnne Flaherty

In this Feb. 11, 2015, file photo, Sen. Dianne Feinstein, D-Calif., speaks during an interview with The Associated about the CIA torture report, in her Capitol Hill office in Washington. Social media giants including Twitter, Yahoo, Facebook and Google are pushing back against Senate legislation that would require them to alert federal authorities of any terrorist activity. The Senate Intelligence Committee has included the requirement in a broader intelligence bill. The House didn't include a similar provision in its bill. (AP Photo/J. Scott Applewhite, File)

Social media giants including Twitter, Yahoo, Facebook and Google are

pushing back against Senate legislation that would require them to alert federal authorities of any terrorist activity, according to industry and government officials.

In private meetings on Capitol Hill, industry officials have told lawmakers and congressional staff that they already ban grisly content like beheadings and alert law enforcement if they suspect someone might get hurt, as soon as they are aware of a threat.

But tech officials also said they worry that the proposed legislation is too broad and would potentially put companies on the hook legally if they miss a tweet, video or blog that hints of an attack. They said the result would probably be a deluge of tips to law enforcement, making it tougher for the government to find more valuable information.

Those interviewed by The Associated Press spoke on condition of anonymity because of the ongoing debate over the legislation.

Sen. Dianne Feinstein, D-Calif., who is backing the legislation, says requiring social media companies to tip off law enforcement to a pending terrorist attack makes sense.

"The FBI and the intelligence community have made it abundantly clear that the terrorist threat is severe and increasing, and that those directing, inspiring and carrying out attacks make heavy use of social media sites," Feinstein told the AP in an emailed statement. "This provision will help get potentially actionable information to the agencies responsible for preventing attacks, without requiring companies to take any steps to monitor their sites they aren't already taking."

The tech industry in 2013 faced a public relations nightmare after former government analyst Edward Snowden leaked details of a massive government surveillance program that relied on their cooperation.

Company officials said the law gave them no choice but to supply consumer data and comply with gag orders that prevented companies from talking about it. Still, many consumers and Internet activists were furious that U.S. businesses had enabled the government to spy on their customers, in some cases even charging the government administrative fees to do it.

Since then, the tech industry has led an aggressive public push to limit surveillance requests and increase transparency, adopting more sophisticated encryption techniques despite opposition from the Justice Department. Their primary argument has been that consumers won't use technology they don't trust, and that unnecessary surveillance would hurt the industry.

At the same time, popular social media sites have become instrumental in helping terrorist groups expand their influence, despite widespread industry policies against posting or promoting terrorist-related content.

The Islamic State group and similar groups have relied heavily on Twitter and Facebook to recruit followers, while militants post beheading videos on sites like Google's YouTube, giving an image the chance to go viral before being shut down. In 2013, al-Shabab live tweeted its Westgate shopping mall massacre, opening up new feeds even after Twitter shut others down.

"This is not your grandfather's al-Qaida," FBI Director James Comey told the Senate Judiciary Committee this month. "This is a group of people using social media to reach thousands and thousands of followers, find the ones who might be interested in committing acts of violence, and then moving them to an (end-to-end) encrypted messaging app."

The same week as Comey's testimony, the Senate Intelligence Committee endorsed Feinstein's proposal that would require companies

that spot terrorist activity on their networks to alert law enforcement.

Feinstein's provision, part of the intelligence authorization bill that still has to be approved by the Senate, is almost identical to the law requiring companies to report child pornography. One exception is that Feinstein's provision doesn't say whether or how a company would be penalized if it fails to report terrorist activity, whereas a tech company can be fined for "knowingly and willfully" failing to report an image of child pornography.

Tech officials say determining what constitutes child pornography is easier to do because the process is more objective. A criminal photograph can be digitally analyzed and assigned a unique identifier that be used to find similar images across networks.

But oftentimes, determining terrorist activity requires more context. The image of an Islamic State flag, for example, could appear in a news article or video clip as well as terrorist propaganda.

Monika Bickert, head of policy management at Facebook, said the social media site shares the government's goal of keeping terrorist content off the site.

"Our policies on this are crystal clear: We do not permit terrorist groups to use Facebook, and people are not allowed to promote or support these groups on Facebook," she said. "We remove this terrorist content as soon as we become aware of it."

The House didn't include a similar provision in its version of the intelligence bill. A spokesman for House Intelligence Committee Chairman Devin Nunes, R-Calif., declined to comment on the issue.

Rep. Adam Schiff, the top Democrat on the House intelligence panel,

said there's "no question" the Islamic State group uses social media to disseminate propoganda and recruit fighters. Schiff, D-Calif., said Congress should work with the tech industry "to determine the most effective response."