

These 26 words 'created the internet.' The US government is coming for them

By [Brian Fung](#), CNN Business. Updated 12:10 PM ET, Tue February 25, 2020

"No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

Washington, DC (CNN Business) For decades, many of the biggest names in tech have leaned on a little-known law to avoid being held responsible for some of the most controversial content on their platforms. The companies have invoked this federal law, known as Section 230 of the Communications Decency Act, in one court case after another to dismiss potentially costly lawsuits over messages, videos and other content created by users.

But now, big changes could be coming to Section 230 that might expose Facebook ([FB](#)), YouTube and others to more lawsuits over hate speech and misinformation for the first time in their histories. If it happens, there could be sweeping repercussions for the internet platforms millions of people use every day.

As social media sites have become hotbeds of hateful, misleading and dangerous content, an increasingly vocal group of critics from government and civil society are pushing for changes to the law. Congress and the Justice Department are now studying the issue: A draft bill by Sen. Lindsey Graham as well as legislation introduced by Sen. Josh Hawley promise to dramatically reshape Section 230, and the DOJ last week held a public workshop to debate the matter.

The push to rethink the law could become the latest flash point between Silicon Valley and the Trump administration. Together with state attorneys general, news publishers and online safety activists, Attorney General William Barr has elevated a campaign to weaken, if not repeal, the law, which dates back to 1996, years before companies like Facebook, Google ([GOOGL](#)) and their peers were founded.

The proposals challenge the deeply held conviction in Silicon Valley that social media companies are just neutral platforms and conduits for information. And they could vastly expand the companies' legal exposure, not only to federal prosecution but potentially state and private lawsuits.

"No longer are tech companies the underdog upstarts," Barr said at last week's Justice Department workshop. "They have become titans of US industry. Given this change in the technology landscape, valid questions have been raised as to whether Section 230's broad immunity is still necessary, at least in its current form."

"The 26 words that created the internet"

The original intent behind Section 230 was to nurture startups and entrepreneurs. One of its key architects, Sen. Ron Wyden, [said as recently as last year](#) that without the law, "all online media would face an onslaught of bad-faith lawsuits and pressure campaigns from the powerful." He's also said Section 230 encourages websites to remove objectionable content by creating a "good Samaritan" expectation: Under the law, tech companies can't be sued for trying to do the right thing, though the federal government can still sue platforms over criminal content.

The seemingly [simple language](#) of Section 230 belies the sweeping impact it's had on the tech industry. Under Section 230, "interactive computer services" are considered legally separate from the users who generate their content. They can't be said to publish or "speak" the words of their users. In practice, courts have repeatedly accepted Section 230 as a defense against claims of defamation, negligence and other allegations. In the past, it's [protected](#) AOL, Craigslist, Google and Yahoo, building up a body of law so broad and influential that Section 230 has come to be [described](#) as "the 26 words that created the internet."

The Internet Association, a major trade group that represents Amazon ([AMZN](#)), Facebook and Google, has called Section 230 a "fundamental pillar" of the modern internet, saying it protects not just tech companies but all groups that offer a space for online communications, including schools, libraries, churches, or neighborhood organizations.

"Section 230 enables services that allows internet users to post their own content and engage with the content of others, whether that's friends, family, co-workers, companies posting jobs, someone posting an apartment for rent, fellow gamers, or complete strangers from the other side of the globe with a shared experience or interest," the association wrote to Barr in a letter last week.

But the immense scrutiny facing Big Tech — on everything from election security to privacy — has created a ripe political environment for questioning Silicon Valley's most important legal shield.

Are tech companies doing enough?

At last weeks' workshop, experts clashed over how much legal responsibility tech companies should bear for hosting malicious content created by its users.

Social media companies say they're improving their ability to detect and take down content that violates their policies. "Section 230 protects the good actors who are cutting off the bad actors," Matt Schruers, president of the Computer & Communications Industry Association, a trade group that represents many large tech companies, said at Wednesday's DOJ event. Without the law's good Samaritan protections, the industry argues, much of that good-faith moderation might end.

Weakening Section 230 could also force websites to vet every piece of content created by their users before it goes online, according to defenders of the law — a task that only large and already powerful players like Facebook may be able to afford. Smaller, competing innovators that could break the grip of Google and Facebook might be snuffed out, said Patrick Carome, a lawyer who has represented tech companies in cases involving Section 230, at last week's event. But critics accuse tech companies of abusing their legal immunity to turn a blind eye to some of the worst content on the internet. These critics allege that powerful online platforms allow harmful material to stay online because it drives engagement — and profit.

"Their financial incentives in content distribution may not always align with what is best for the user," Barr said at the event.

To help drive the message home, the Justice Department has turned to child abuse experts who say companies like Facebook must bear responsibility for the child pornography and sexual predators that lurk on its platform.

Facebook said it [took action](#) against more than 24 million pieces of child exploitative content last year. Most of it, the company has said, was caught automatically by Facebook's filters and that "we remove much of this content before people see it."

Despite those successes, child sexual abuse content is still a widespread problem, said Yiota Souras, general counsel for the National Center for Missing and Exploited Children, at Wednesday's event. Last year, the non-profit group received about [17 million reports](#) of online child exploitation, including over 15 million linked to Facebook, nearly half a million concerning Google and tens of thousands related to Microsoft, Imgur and Snapchat, among others.

One proposal backed by state attorneys general would amend Section 230 by giving them the power to sue platforms for hosting child abuse material, just like the federal government can. "We'll clean up your industry, instead of waiting for your industry to clean up itself," said Doug Peterson, Nebraska's attorney general, at the DOJ workshop.

A fierce debate heats up over the future of the internet

The Section 230 debate is tied to another politically charged tech issue: encryption, the technology that secures many everyday transactions ranging from iMessages to credit card swipes to sensitive business and government databases.

Souras said online child exploitation will only get worse if Facebook moves ahead with plans to encrypt all messages on its platforms, scrambling their contents so that not even the company knows what child abusers may be saying — and to whom — in private.

The thought of bad actors "going dark" has long been a fear of the FBI, which has asked companies like Apple for help decrypting the secure data of criminal suspects. But Apple and the tech industry have resisted. They've argued that giving the authorities a special way to tap into encrypted communications will encourage hackers and foreign adversaries to exploit the same tool. If that happens, it could ultimately weaken digital security for millions of Americans.

Some legal experts worry the Trump administration's push to impose new rules on tech companies could lead to broad expansions of government power. Those perceptions were reinforced earlier this month when Sen. Graham's draft bill on Section 230 began circulating around Washington.

The bill seeks to withhold Section 230's legal protections from tech companies unless they agree to implement "best practices" that would be designed by a commission and ultimately approved by the attorney general.

Technology and legal experts slammed the bill, saying it would give Barr a blank check to write his own regulations designed to weaken encryption, expand domestic surveillance, and force tech companies to undermine user security using the threat of lawsuits. In other words, the deep, longstanding divide over encryption between tech and government may be driving some of the recent conversation around content policy.

"Barr is cynically exploiting [child sexual abuse material] as a pretext for attacking the privacy of law-abiding Americans who would benefit from having secure communications tools," said Berin Szoka, president of the Washington-based think tank TechFreedom.