

OPINION

Why Section 230 hurts kids, and what to do about it

It wasn't supposed to be this way.

The smartphone and the internet are revolutionary inventions, but in the absence of rules and responsibilities, they threaten the greatest invention of the modern world: a protected childhood. | Photo: Leonardo Fernandez Vilorio/Getty Images

Bruce Reed**James P. Steyer**

December 8, 2020

Mark Zuckerberg makes no apology for being one of the least-responsible chief executives of our time. Yet at the risk of defending the indefensible, as Zuckerberg is wont to do, we must concede that given the way federal courts have interpreted telecommunications law, some of Facebook's highest crimes are now considered legal. It may not have been against the law to livestream the massacre of 51 people at mosques in Christchurch, New Zealand or the suicide of a 12-year-old girl in the state of Georgia. Courts have cleared the company of any legal responsibility for violent attacks spawned by Facebook accounts tied to Hamas. It's not illegal for Facebook posts to foment attacks on refugees in Europe or try to end democracy as we know it in America.

On the contrary, there's a federal law that actually protects social media companies from having to take responsibility for the horrors that they're hosting on their platforms. Since Section 230 of the 1996 Communications Decency Act was passed, it has been a get-out-of-jail-free card for companies like Facebook and executives like Zuckerberg. That 26-word provision hurts our kids and is doing possibly irreparable damage to our democracy. Unless we change it, the internet will become an even more dangerous place for young people, while Facebook and other tech platforms will reap ever-greater profits from the blanket immunity that their industry enjoys.

It wasn't supposed to be this way. According to former California Rep. Chris Cox, who wrote Section 230 with Oregon's Sen. Ron Wyden, "The original purpose of this law was to help clean up the internet, not to facilitate people doing bad things on the internet." In the 1990s, after a New York court ruled that the online service provider Prodigy could be held liable in the same way as a newspaper publisher because it had established standards for allowable content, Cox and Wyden wrote Section 230 to protect "Good Samaritan" companies like Prodigy that tried to do the right thing by removing content that violated their guidelines.

But through subsequent court rulings, the provision has turned into a bulletproof shield for social media platforms that do little or nothing to enforce established standards. As Jeff Kosseff wrote in his book "The Twenty-Six Words That Created the Internet," the provision "would come to mean that, with few exceptions, websites and internet service providers are not liable for the comments, pictures, and videos that their users and subscribers post, no matter how vile or damaging."

Facebook and other platforms have saved countless billions thanks to this free pass. But kids and society are paying the price. Silicon Valley has succeeded in turning the internet into an online Wild West — nasty, brutal, and lawless — where the innocent are most at risk. The smartphone and the internet are revolutionary inventions, but in the absence of rules and responsibilities, they threaten the greatest invention of the modern world: a protected childhood.

Since the 19th century, economic and technological progress enabled societies to ban child labor and child trafficking, eliminate deadly and debilitating childhood diseases, guarantee universal education and better safeguard young children from exposure to violence and other damaging behaviors. Technology has tremendous potential to continue that progress. But through shrewd use of the irresponsibility cloak of Section 230, some in Big Tech have turned the social media revolution into a decidedly mixed blessing.

Although the U.S. has protected kids by establishing strict rules and standards on everything from dirty air and unsafe foods to dangerous toys and violence on television, the internet has almost no rules at all, thanks to Section 230. Kids are exposed to all manner of unhealthy content online. Too often, they don't even have to seek it out; harm comes looking for them. Social media platforms run inappropriate ads alongside content that kids watch. Platforms popular with

children are overrun with advertising-like programming, such as unboxing and surprise videos.

Because their business model depends on commanding as much consumer attention as possible, companies push content to kids to keep them on their platforms as long as possible. All the tricks of manipulative design that make Big Tech dangerous for society — autoplay, badges and likes — put young people at the greatest risk. In the early days of the web, a *New Yorker* cartoon showed a dog at a desktop, with the caption, "On the internet, nobody knows you're a dog." On today's internet, nobody cares if you're a kid.

Exhibit A: YouTube

Big Tech's browse-at-your-own-risk ethos is particularly evident on sites like YouTube, where kids are doing exactly what they've done for more than half a century — staring at a screen — with one key difference: There are no longer any limits on what they can watch. Google's algorithms profess to know everything we desire, but they certainly don't know what we want for our children. In fact, grown-ups are currently leading a wave of nostalgia for America's golden age of children's entertainment: "Sesame Street" celebrated its 50th anniversary; Tom Hanks starred as Mr. Rogers in a critically-acclaimed movie; and the launch of Disney+ turned Disney's vast library of animated and adventure classics into the most successful streaming service of all time.

Such nostalgia is both understandable and ironic when today's young kids are watching YouTube, an online channel that admits it's not appropriate for children under 13. A Pew Research Center survey found that four out of five parents with children age 11 or younger let them watch YouTube, and a third of them watch regularly. Meanwhile, three out of five YouTube users say they come across "videos that show people engaging in dangerous or troubling behavior." Likewise, three out of five parents who let their young children watch YouTube say they encounter content "unsuitable for children." As the channel's proud parent Google has routinely boasted to advertisers, YouTube is "the new 'Saturday morning cartoons'" and "today's leader in reaching children age 6-11 against top TV channels."

What might kids find on YouTube? YouTube videos aimed at kids have shown all manner of violence and perversion, from Peppa Pig armed with guns and knives to sex acts with Disney characters like Elsa. The Maryland couple behind

FamilyOFive, a once-popular, now-terminated YouTube channel that attracted over 175 million views, posted viral prank videos of child abuse perpetrated against their own children. Perhaps most troubling: YouTube's behavioral algorithms appear to steer children into harm's way.

An exhaustive research study funded by the European Union found hundreds of disturbing videos, with hundreds of thousands of views, aimed at children between the ages of 1 and 5. The report concludes, "Young children are not only able, but likely to encounter disturbing videos when they randomly browse the platform starting from benign videos." Kids are growing up in the darkest age of children's entertainment in American history. As technology writer James Bridle warned in 2017, "Someone ... is using YouTube to systematically frighten, traumatize, and abuse children, automatically and at scale, and it forces me to question my own beliefs about the internet, at every level."

The YouTube saga shows the folly of self-regulation when the laws aren't just weak but actually immunize companies from accountability for their behavior. Section 230 not only fails to protect kids from disturbing content, but it also limits the effectiveness of other child-protective laws.

In 2019, the Federal Trade Commission and the New York attorney general went after Google for violating the Children's Online Privacy Protection Act, which is supposed to prevent companies from collecting information from and personally targeting kids under 13. For all its limitations, COPPA was intended to give parents peace of mind and create a walled garden in which children could not be preyed upon. Section 230 is a bulldozer that knocks those walls down, enabling platforms that profit off kids to avoid taking full responsibility for their actions. Many platforms skirt those provisions by claiming they do not have "actual knowledge" that users are under 13, as the law requires — even though they can usually gauge users' age from their online behavior. Google escaped by agreeing to a modest \$170 million fine.

What to do about it

How can America revoke Big Tech's free pass before it's too late? First, we must set aside the industry's self-serving defense of Section 230. Platform companies insist that if they have to play by the same rules as publishers, individuals' right of free speech will vanish.

But treating platforms as publishers doesn't undermine the First Amendment. On the contrary, publishers have flourished under the First Amendment. They have centuries of experience in moderating content, and the free press was doing just fine until Facebook came along. Section 230 is more like the self-protection that gun manufacturers — the only other industry in America with broad legal immunity — extorted from Congress under the pretense of the Second Amendment. The Protection of Lawful Commerce in Arms Act of 2005, passed just as the federal assault weapons ban expired, protects gunmakers from liability for crimes committed with their products. Hunters and gun owners don't benefit from that law, but it has unleashed the gun industry to sell millions of assault rifles with impunity.

The tech industry's right to do whatever it wants without consequence is its soft underbelly, not its secret sauce. Admitting mistakes is the sector's greatest failing; taking responsibility for those mistakes is its gravest fear. Zuckerberg leads the way by steering into every skid. Instead of acknowledging Facebook's role in the 2016 election debacle, he slow-walked and covered it up. Instead of putting up real guardrails against hate speech, violence, and conspiracy videos, he has hired low-wage content moderators by the thousands as human crash dummies to monitor the flow. Without that all-purpose Section 230 shield, Facebook and other platforms would have to take responsibility for the havoc they unleash and learn to fix things, not just break them.

Congress never intended to give platforms a free pass. As Jeff Kosseff, the law's self-proclaimed biographer, points out, Congress enacted Section 230 because "it wanted the platforms to moderate content." So the simplest way to address unlimited liability is to start limiting it. In 2018, Congress took a small step in that direction by passing the Stop Enabling Sex Traffickers Act and the Allow States and Victims to Fight Online Sex Trafficking Act. Those laws amended Section 230 to take away safe harbor protection from providers that knowingly facilitated sex trafficking.

Congress could continue to chip away by denying platform immunity for other specific wrongs like revenge porn. Better yet, it could make platform responsibility a prerequisite for any limits on liability. Boston University law professor Danielle Citron and Brookings Institution scholar Benjamin Wittes have proposed conditioning immunity on whether a platform has taken reasonable efforts to moderate content. In their article they note that "perfect immunity for platforms deliberately facilitating online abuse is not a win for

free speech because harassers speak unhindered while the harassed withdraw from online interactions." Citron argues that courts should ask whether providers have "engaged in reasonable content moderation practices writ large with regard to unlawful uses that clearly create serious harm to others."

Demanding reasonable efforts to moderate content would represent progress. But that is a dangerously low bar for an industry whose excuse for every failure has been "sorry, we'll do better next time." A social media platform like Facebook isn't some Good Samaritan who stumbled onto a victim in distress: It created the scene that made the crime possible, developed the analytics to prevent or predict it, tracked both perpetrator and victim and made a handsome profit by targeting ads to all concerned, including the hordes who came by just to see the spectacle.

Washington would be better off throwing out Section 230 and starting over. The Wild West wasn't tamed by hiring a sheriff and gathering a posse. The internet won't be either. It will take a sweeping change in ethics and culture, enforced by providers and regulators. Instead of defaulting to shield those who most profit, the United States should shield those most vulnerable to harm, starting with kids. The "polluter pays" principle that we use to mitigate environmental damage can help achieve the same in the online environment. Simply put, platforms should be held accountable for any content that generates revenue. If they sell ads that run alongside harmful content, they should be considered complicit in the harm. Likewise, if their algorithms promote harmful content, they should be held accountable for helping redress the harm. In the long run, the only real way to moderate content is to moderate the business model.

In 2019, before Patrick Crusius massacred 23 people in an El Paso Walmart, he wrote a four-page white supremacist manifesto decrying a "Hispanic invasion of Texas." Like John Timothy Earnest — the disgruntled anti-Semite who opened fire on a synagogue in Poway, California, the same year — Crusius posted his racist thoughts on an online message board called 8chan. In March 2019, the shooter in Christchurch, New Zealand, livestreamed his killing spree for 17 minutes on social media for millions to see. All three of those attacks, and others like them, spread across the globe, inciting violence, glorifying white supremacy and aggrandizing murderous young men intent on passing the torch of hate onto the next generation.

One crucial difference sets the Christchurch incident apart. In the wake of the El Paso and Poway shootings, Washington did what it has done so many times before: nothing. But New Zealand Prime Minister Jacinda Ardern won the world's heart by not only banning the military-style assault weapons the shooter used but by setting out to take away his other weapon: the spread of extremist content online. She challenged leaders of nations and corporations around the world to join the Christchurch call to action to make sweeping changes in laws and practice to prevent the posting and to hasten the removal of hateful, dangerous content on social media platforms. New Zealand could reform its gun laws, but, she said, "we can't fix the proliferation of violent crime online by ourselves."

In the end, Section 230 of the Communications Decency Act is no longer a necessary evil that nascent internet companies depend on to thrive. Instead, it has become our collective excuse not to take away the platform that hate depends on to grow and spread. The longer we do nothing, the more our humanity looks stripped, beaten and half-dead on the side of the road. Our kids know the moral to the story: Good Samaritans would stop to help the victim. So should we.