Written Testimony of Carrie Goldberg

Founder, C. A. Goldberg, PLLC

Before the U.S. House of Representatives

Committee on Energy and Commerce

Subcommittee on Communications and Technology

"Legislative Proposal to Sunset Section 230 of the Communications Decency Act"

May 22, 2024

Chair McMorris Rodgers, Ranking Member Pallone and distinguished members of the House Subcommittee on Communications and Technology. Thank you for inviting me to testify today and allowing me to share my experiences representing victims of catastrophic injuries caused by online platforms and the heartbreak of my clients being denied justice because they are locked out of the courts by an obsolete law, Section 230 of the Communications Decency Act.

My name is Carrie Goldberg. I founded the law firm C.A. Goldberg, PLLC to represent victims of catastrophic injuries – people who've had their privacy invaded, bodies raped, freedoms enslaved, and sometimes lives snuffed out entirely. In the majority of my cases, well over a thousand now, my clients' injuries were facilitated by tech companies. The people -- victims of child sexual exploitation, cyberstalking, trafficking, corporate facilitated suicide -- hire me as their lawyer expecting me to avenge their damages. The worst part of my job, though is telling people who've suffered horrific nightmares that Congress took away their right to justice. *We can't sue*, I tell them, *Congress passed a law in the 90's that lets tech companies get away with what they did to you*.

Yes, the law was drafted narrowly when the internet was nothing like today's. When platforms really were just publishers and the harms were limited to defamation. But in the 28 years, our courts have applied old precedent to new products, acting as though complex tech products with incredible sophistication like AI, algorithms, geolocation, virtual reality – are the same as a Prodigy bulletin board.

Today I testify in support of the Sunset Clause.

Since I was last here testifying in Dec 2021, I have won four motions to dismiss in cases where platforms have declared immunity – twice in *A.M. v Omegle* (No. 3:21-cv-01674-MO, 2023 WL 1470269 D. Or.) where the platform was defective and engaged in trafficking by matching adults and children for livestreaming, in *Neville v. Snap* (Case No. 22STCV33500 (Cal. Superior Ct)) where the platform was defectively designed and negligent for facilitating the sale of fentanyl-laced drugs to children, and in *re Soc. Media Adolescent Addiction/Pers. Inj. Prod. Liab. Litig.* (No. 4:22-MD-03047-YGR,

2023 WL 7524912 (N.D. Cal.)) where platforms YouTube, Instagram, Facebook, Snap, and TikTok were accused of designing addictive algorithms causing self-harm, mental health disorders, sexual exploitation, eating disorders, and suicides to children.

But, as I will discuss below, courts continue to immunize tech companies for some of the most serious harms, ignoring precedent, statute, and common-sense.

Congress created Section 230. From the fortifications of this law has grown the most wealthy, omniscient, omnipotent industry in the history of the world, an industry that tramples the individual.

The common law's precedent-based court system is intended to promote stability, consistency, and equity across the U.S. court system. The dilemma is that reliance on past decisions can also sometimes perpetuate injustice. This could be no more true than with a law that was drafted for one sort of technology – comparatively unsophisticated text-based message boards back when the internet was accessible on desktops using modems people paid a monthly subscription for and only 0.4% of the world population used it. Today's technology of course is far more sophisticated with limitless ability to harm. No longer are harms limited to defamation that only a few unknown strangers might see. Now the internet can overturn elections, spur genocides, coordinate government takeovers, corporatize suicide, spawn unrivaled increases in teen depression, self-harm, and eating disorders.

Sweeping language from early cases involving primitive text-based online service providers has been used to throw out cases today. For instance, a throwaway line in the 1996 case Zeran v AOL, the 4th Circuit had a throwaway line about how Section 230 immunizes an online service provider for "**any cause of action** that would make service providers liable for information originating with a third-party user of the service." [emphasis added]. From that, spawned the but-for theory which continues to prevail in many places to this day.[1] As the theory goes, never mind whether a service

[1] See e.g. *Herrick v Grindr, LLC,* 765 F. App'x 586, 590-91(2d Cir. 2019) (applying a but-for test to dismiss claims that Grindr was defectively designed by lacking technology to remove a stalker who sent 1000+ men to the plaintiff's home to rape him); *Doe v Grindr, LLC (US Ct. of App. 9th Circuit 24-0475), {*applying a but-for test to dismiss claims involving child-rape where the product was marketed to children); *United States v Stratics Networks Inc.,* No. 23-cv-0313-BAS-KSC, 2024 WL 966380, at *14 (S.D. Cal. Mar. 6, 2024) (applying a but-for test to prohibit a Telephone Consumer Privacy Act suit against a company that helps telemarketers evade consumer protection laws); *United States v. EZ Lynk Sezc,* No. 21-cv-1986 (MKV), 2024 WL 1249224, at *9-12 (S.D.N.Y. Mar. 28, 2024) (applying a but-for test to prohibit enforcement of the Clean Air Act against a company that helps drivers defeat emissions controls on vehicles); *McCarthy v Amazon.com*, (US Ct. of App. 9th Circuit No. 23-35584) (applying a but-for test to dismiss liability of a product seller of suicide kits where a fact in the complaint mentioned the manipulation of user reviews; *Dennis v. MyLife.com, Inc.,* No. 20-cv-954, 2021 WL 6049830, at *6-7 (D.N.J. Dec. 20, 2021) (applying a but-for test to dismiss a claim based on a clear Fair Credit Reporting Act violation.)

provider was actually acting in the capacity of a publisher, if the harm originates from content, the platform should be immune for all claims. The Zeran case is so old that it actually defines "the Internet" in footnote 1 of the trial court decision.[2]

Perversely, even back in 1996, one year after the CDA went into effect, the Zeran trial court recognized that Congress would need to provide tune-ups to the CDA as the technology developed: "[T]he Internet is a rapidly developing technology – today's problems may soon be obsolete while tomorrow's challenges are, as yet, unknowable. In this environment, Congress is likely to have reasons and opportunities to revisit the balance struck in CDA."

One of the earliest cases applying the *Zeran* precedent to a case of extreme harm was where a man filmed himself forcing sexual acts between three young boys and then used AOL chatrooms to market the photographs. The 11-year-old plaintiff's mom alerted AOL about the child abuser and how he was using its platform to distribute the child pornography but they refused to intervene. *Doe v AOL* was originally brought in 1997 and thrown out in 2001 because of Section 230. The incredulous dissenting judge proclaimed that "it is inconceivable that Congress intended the CDA to shield from potential liability an ISP alleged to have taken absolutely no actions to curtail illicit activities . .. despite actual knowledge that a source of child pornography was being advertised and delivered. . .while profiting from its customer's continued use of the service.[3]"

---

[2] "'The Internet', as the term is used here, refers to the immeasurable network of computers interconnected for the purpose of communication and information exchange. This network can be accessed in a variety of ways, including through commercial 'online services' such as American Online, Inc. These commercial services offer access to their own computer network and organizational software allowing subscribers to interconnect easily with computer networks other than those proprietary to the 'online service.'" *Zeran v America Online, Inc. D.VA 96-952-A.*

[3] "Given the precise, limiting language of the statute, the stated policy underlying the CDA, and the CDA's explicit legislative history, it is inconceivable that Congress intended the CDA to shield from potential liability an ISP alleged to have taken absolutely no actions to curtail illicit activities in furtherance of conduct defined as criminal, despite actual knowledge that a source of child pornography was being advertised and delivered through contact information provided on its service by an identified customer, while profiting from its customer's continued use of the service. Such an interpretation transforms a statute intended to further and support responsible ISP efforts to protect children and the public from even questionably harmful and illegal materials into a statute which both condones and exonerates a flagrant and reprehensible failure to act by an ISP in the face of allegedly specific, known dissemination of material unquestionably harmful to children.[23] In my view, the interpretation adopted today provides a foundation for far-ranging forms of illegal conduct (possibly harmful to society in far different ways) which ISPs can, very profitably and with total immunity, knowingly allow their customers to operate through their Internet services. I fear that the blanket immunity interpretation adopted by the

Since its inception, judges pleaded with Congress to return to Section 230 to fix it. Yet besides one clarification in 2018, Congress has been entirely hands-off.

Congress created Section 230. People can disagree on whether the experiment was a success or not. But we have reached the experiment's conclusion. And now, the onus is on Congress to fix the disaster unraveling before us with an entire unregulated industry that's been legislated out of our courts' grasp.

We are here to restore balance. With the Sunset Clause, we show that no industry is outside the reach of our justice system when Americans are harmed.

I. My clients' cases dismissed under Section 230

A. Immunity for distributing suicide kits

McCarthy, et al., v Amazon.com (Pending in the 9th Circuit)

In February 2021, I was hired by Ruth Scott. Two months prior, her only child, Mikael, had discovered a pro-suicide website where people could encourage each other to die and they could live-post it. Users on the site recommended a specific chemical for sale on Amazon, Sodium Nitrite, that was only twenty dollars, and ensured a fast death delivered to your doorstep. Indeed, a teaspoon of the powder mixed with water ends a life in about 20 minutes. On Amazon's website I saw pictures of the product and lots of user reviews from heartbroken parents and toxicologists saying the product had killed their kid.

I expected the case to just be a pro bono letter. Surely Amazon was just too big to realize it was selling a suicide kit. And I say kit, because it recommended that users who purchase the chemical also buy attending products to guarantee death – including a small scale to measure the dose, Tagamet anti-emetic pills to prevent vomiting, and an Amazon edition suicide manual with an entire chapter on how to die from Sodium Nitrite. Mikael had also the scale and Tagamet was found in his room.

Unlike the other products Amazon sells, the 99% pure Sodium Nitrite it sold to Mikael has no household use. [Contrast to curing salts which are 6% pure and dyed pink for safety because even that purity is dangerous].

To my surprise, when Amazon's lawyers responded in May, rather than taking the product off the market, they doubled down and said they have no duty to restrict sales just because somebody was "misusing." They said they could not be held liable anyway.

---

majority today thrusts Congress into the unlikely position of having enacted legislation that encourages and protects the involvement of ISPs as silent partners in criminal enterprises for profit. Confident that Congress did not intend such an incongruous result, I respectfully dissent." – Judge J. Lewis *Doe v. America Online Inc.* (2001) Supreme Court of FL No. SC94355

I ended up suing Amazon. And other parents joined the fight. I now represent 24 families to whom Amazon knowingly sold this chemical. We have six cases filed. One of the cases is on behalf of the families of a 16 year old girl, Kristine Jónsson from Ohio and 17 year old Ethan McCarthy from West Virginia

In that case, I sued saying that Amazon was negligent for selling and distributing Sodium Nitrite when it knew that the product was regularly used for death. I explained in the long pleadings all the different sources of Amazon's knowledge that it was selling the chemical – including it receiving a letter from Congress demanding answers. I explained that Amazon removed one-star reviews to manipulate the ranking of the product and suppressed the warnings that parents left.

The lawsuit sues Amazon for its role as a seller – not as a platform. It was a basic seller negligence case. But the judge said that since I had mentioned user reviews – i.e. content posted by another user, Section 230 applied and the claim should be thrown out. This was one sentence in a 42 page complaint and none of the claims even relied on that fact. The Court dismissed the case with prejudice and said Amazon was immune from liability for intentionally concealing the harms connected to the product because the lawsuit included language that discussed the posting of third party content.

B. Immunity for marketing a hook-up app to children

John Doe v Grindr (Pending in the 9th Circuit)

Grindr is the world's biggest hook-up app for LGBTQ+ individuals. In recent years, it has begun campaigns on TikTok and Instagram clearly marketed to children. Not only are these platforms primarily used by children, but the content Grindr posted showed videos of adolescent-appearing kids in school gymnasiums and high school or middle school settings.

In April, 2019, John Doe, a closeted 15 year old gay boy living with Autism and ADHD in a rural community fell victim to Grindr's juvenile-targeting marketing. He was desperate to meet other gay kids and naively thought he could find friends on Grindr. Without his parent's knowledge or permission, he downloaded the app, complied with a prompt that told him he needed to be 18 or older and created a profile, choosing whatever birthday he wanted. Grindr extracted John Doe's location data from his phone and offered proximately located users to him and offered him to nearby adults. The day he downloaded Grindr, he matched with an adult nearby his school, met up with him and was raped. Stunned, traumatized, and confused, Doe returned to Grindr. Over four consecutive days in total, Grindr matched Doe with four adults, each who raped him with varying degrees of force and violence. Three of the four were criminally convicted. Doe experienced significant trauma and distress from the rapes, causing him to attempt suicide, drop out of school, and require inpatient hospitalization.

On March 10, 2023, Doe sued Grindr under theories of strict products liability, negligence, and trafficking. He alleged that Grindr breached its duty of care by aggressively marketing to children and then matching them with adults. Grindr alleged

that it is but a forum for "speech." The District Court dismissed the entire case with prejudice, claiming that but-for the user content, none of the harms that befell Doe would have occurred. The judge lamented that "[t]he facts of this care are indisputably alarming and tragic. No one should endure what Plaintiff has." Yet, he dismissed the case because, according to the Court, Section 230 immunizes the platform because if not for user content – specifically the location data Grindr extracts from users to match them with other users – none of the harms would have happened to Doe. The trafficking claims were dismissed because the judge said that Grindr merely "turned a blind eye" to the unlawful conduct, which it is allowed to do.

The case is currently on appeal in the Ninth Circuit.

C. Immunity for Extreme Stalking the Platform Knew About

Matthew Herrick v Grindr (dismissed with prejudice, 2nd Circuit)

Starting in October 2016, 33-year-old Matthew Herrick began receiving unwanted strangers at his home and work. Sometimes as many as 33 in a day. Matthew knew his ex was behind the strangers – they began showing up a week after their break-up. The impersonating profiles sent men for fisting, orgies and aggressive sex. In the direct messages, the strangers were told that Matt's resistance was part of the fantasy. Matthew had tried everything he could to take care of the problem on his own. He filed more than a dozen complaints with his local police precinct.

In all, about 50 separate complaints were made to the company reporting the fake profiles, either by Matthew or on his behalf. The only response the company ever sent was an automatically generated email: "Thank you for your report." Over the course of ten months more than 1,400 men, came to his home and workplace expecting sex.

Even though Grindr's terms of service state that Grindr can remove any profile and deny anybody the use of their product at the company's discretion, they refused to help. After Matthew's approximately 50 pleas to Grindr for help were ignored, we sued Grindr in New York State Supreme Court, New York County, and obtained immediate injunctive relief requiring that Grindr ban the malicious user.

It's not clear exactly how Grindr was so easily being used to send the strangers to Matthew—it might have been through a spoofing app that worked with Grindr's geolocation software or something more technical. But the strangers who came to Matthew said they were sent through the Grindr app and would show Matthew the fake profiles with his pictures, geolocation maps showing how far away they were from Matthew, and direct messages telling them which buzzer to ring and what kind of sex Matthew was eager to have.

We sued Grindr under product liability theories. Grindr is a defectively designed and manufactured product insofar as it was easily exploited—presumably by spoofing apps available from Google and Apple—and didn't have the ability, according to the courtroom admissions of Grindr's own lawyers, to identify and exclude abusive users.

For a company that served millions of people globally and used geolocating technology to direct those people into offline encounters, it was an arithmetic certainty that at least some of the time the product would be used by abusers, stalkers, predators and rapists. Failing to manufacture the product with safeguards for those inevitabilities, I argued, was negligent.

The SDNY judge dismissed the claim with prejudice declaring that Grindr was immune from liability pursuant to the Communications Decency Act, because according to her, our claims depended on information provided by another information content provider. If not for Matthew's ex using the app, she reasoned, none of this would have happened to Matthew. She reduced all the harm as flowing from the ex's actions, not Grindr's, and therefore reasoned that the company was immune from liability and had no obligation to Matthew.

We appealed to the Second Circuit repeating the argument that because we were suing Grindr for its own product defects, operational failures and broken promises in their terms of service—and not for any content provided by Matthew's ex—Grindr was not eligible to seek safe harbor from Section 230. To rule against Matthew would set a dangerous precedent, establishing that as long as a tech company's product was turned to malicious purposes by a user, no matter how foreseeable the malicious use, that tech company was beyond the reach of the law and tort system.

On March 27, 2019 the Second Circuit issued a summary order affirming the district court's dismissal of the complaint. On April 11, we filed a petition for panel rehearing, or, in the alternative, for rehearing *en banc*. On May 9, that too was denied. In October 2019, our writ for certiorari to the Supreme Court, also was denied. It was the end of the road for *Herrick v Grindr*.

In 2020 Justice Clarence Thomas wrote a dissent to a writ for certiorari in the case *Malware Bytes, Inc. v Enigma Software Group*. He lamented that when Congress enacted Section 230, most of today's major Internet platforms did not exist. Then he condemned how the two and a half decades of lower court decision "eviscerated the narrow liability shield" Congress had intended. Making his point, he cited Matthew's case, furious that courts so extravagantly interpreted Section 230 that it even granted immunity in a product liability case "concerning a dating application that allegedly lacked basic safety features to prevent harassment and impersonation."

II. Section 230, how we got here

In 1995, Congress passed 47 U.S.C. Section 230 as part of the Communications Decency Act. It was a small section of the 96 Telecom Act which was mostly focused on telecom issues like local phone service. Section 230 established protections for websites from being sued for publication torts like defamation for content their users post. At the time, the main source of user-generated content was online bulletin boards, Prodigy, Compuserve, and AOL, where the most heinous acts of the day, comparatively mild to the destruction now, were people calling each other frauds. One court had found that a

bulletin board was liable for defamatory content one user posted about another, because that bulletin board had been actively moderating the content on its site.

In the mid-1990's haze of deregulation, Congress speculated that if bulletin boards were freed from liability to their users, they'd self-moderate and voluntarily implement measures to keep their platforms and users safe. The idea was that removing the threat of liability would *incentivize* these companies to be good Samaritans and self-govern their platforms responsibly.

That is not what happened. Just as when Wall Street was deregulated, without rules, regulation or the threat of lawsuits from injured users, the companies ran amuck. They could grow at quantum speed without the need to invest any money into keeping their product safe or establishing responsible policies and procedures to respond to injuries or staffing moderators in scale with the number of users on their platforms. Rather than incentivizing good content moderation hygiene, Section 230 became a shield for platforms, and a license to get away with no content moderation or safety measures.

Concurrently, an overhaul of internet companies' revenue model – from subscription to "free" -- was the nail in the coffin for online consumer safety. What had once been subscription-based model with users paying monthly fees to companies like AOL in the 90's transformed into an advertisement-based model. Users were no longer the customers; advertisers were. No longer did companies need to compete to provide the best service to their users. When Internet products became "free" to users, users went from being valued customers to the commodity, the eyeballs on the ads. The cold shoulder to users' needs and safety has become far more extreme in today's internet where users are not just the commodity to advertise at, but instead are the raw material from which companies like Facebook, Google, and Amazon extract behavioral and consumer data, then use it to manipulate and forecast those very same users' habits.

Ironically, my clients, especially my exploited underage clients, are the ones that the 1995 Congress was trying to protect. Yet, this is the population most victimized by the creep of immunity.

Over the past 28 years, our courts took a rather narrowly written law which was intended only to prevent lawsuits against tech companies related to publication torts, like defamation and metastasized it into shielding the most powerful companies in the world from responsibility for things like terrorism, genocide, child sexual exploitation, illegal firearms dealing, and stalking. It expanded the law well beyond claims of defamation, to also throw plaintiffs out of court if they claimed their injuries were caused by negligence, fraud, contract breaches from companies violating the terms of service agreements, discrimination in advertisements, and the product being detective. Even statutory damages in our federal child pornography law is off-limits for survivors despite companies making a profit off their nude images.

The tech industry is not inherently bad. As David Michaels explains in his book, "The Triumph of Doubt" about cover-ups in toxic torts, most problematic corporate behavior happens through a series of small decisions. Publicly traded and investor-based

companies are pressured to deliver growing profits on a short-term basis. The culture of angel investors and venture capitalists hungry for that next unicorn normalizes this dangerous "move fast and break things" ethos. Unfortunately, the broken things are too often living breathing humans. Milton Friedman's fetishized model that a corporation's primary objective is to maximize shareholder value, even presenting it as a fiduciary responsibility limited only by the boundaries of law and regulation. So when there's neither law nor regulation, and the injured are excluded from our courts to vindicate their harms, the products get more dangerous and the corporate greed more deeply rooted.

The importance of litigation to discourage corporations, entire industries even, from their most antisocial temptations. When the ill effects of a dangerous or toxic product shift the true costs of those products onto humans and communities, litigation is how we boomerang those costs right back to the source. This "regulation by litigation" is how our society took on Big Tobacco, opioid manufacturers, asbestos, carcinogenic weedkillers, massive polluters, and more. The process of litigation, even when the defendants engaged in evasion, obfuscation, and cover-ups have provided critical inside reports and insights into the level of recklessness with which the industries knew they were injuring the community. Without litigation, we must rely on the whitewashed dribs and drabs of "transparency reports" that tech PR flacks deign to release to the public or wait for a rare whistleblowers like Frances Haugen to leak internal documents at tremendous personal risk.

III. Removing Section 230 immunity will not flood the courts.

Removing the exemption of liability will not result in a groundswell of litigation. In discussing Section 230 reform, some people erroneously claim changes to 230 will "create liability" for tech companies. This is incorrect. Removal of immunity will not make defendants liable for online harms. Instead, it just means plaintiffs have a chance to plead and prove their claims in the first place. Fears that tech companies will be overwhelmed with litigation are unfounded and frankly, reveal the fearmonger's unfamiliarity with how litigation works. Many of the staunchest defenders of Section 230 seem to think that *all* lawsuits are frivolous. These people seem to take issue with consumer protection laws and the United States tort system in general. In this section I discuss why we need not fear a stampede to the courthouse.

The onus is on the plaintiff to plead and prove liability.

Many people say that elimination of Section 230 will "create liability" for platforms. Wrong. Eliminating Section 230 does not *create* liability. Instead, it removes the roadblock that prevented plaintiffs from even alleging liability. "The fact that [an ISP's] actions are not immune under Section 230 does not necessarily mean they were tortious." *Ziencik, et al. v. Snap*, No. 21-7292, 2023 WL 2638314 (C.D. Cal. Feb. 3, 2023 Like all litigation, the onus is on the plaintiff to plead and prove the merits of the case. The adversarial system provides extensive opportunity for defendants to show the

plaintiff failed to plead a claim or cannot prove the defendant is responsible. The process begins with plaintiffs needing to satisfy the harsh pleading standards required of federal cases per *Iqbal* and *Twombly*. The plaintiff must have an actual cause of action to plead and then must plausibly plead each element. For instance, if pleading negligence, the plaintiff must plead that there's a relationship between the plaintiff and the defendant, that the relationship created a special duty on defendant, that defendant breached that duty, that plaintiff suffered an injury, and that the defendant's breached duty was the proximate cause of the injury. The rigorous litigation stages of discovery, motion practice, and trial are as cumbersome – if not more – on the plaintiff to prove their case as the defendant.

Rules against frivolous lawsuits

Rule 3.1 of the Model Rules of Professional Conduct forbids an attorney from bringing frivolous lawsuits. Attorneys have a duty to not file meritless cases. Both the client and the attorney can be sanctioned for bringing meritless claims.

Basic economics deter low injury cases

Proving liability is an arduous, laborious, years-long and expensive undertaking for plaintiffs and/or their attorney. Economic drivers separate the wheat from the shaft. Personal injury cases are almost always taken on contingency. Discovery, expert witnesses, depositions, and thousands of hours of lawyer time adds up. Likewise, attorneys working on contingency with their own profit and loss concerns do not take cases unless the upside justifies the risk of losing litigation. Consequently, low injury are not affordable as a business model when the cost of the litigation exceeds the amount recoverable to the client.

Having facts that satisfy all elements for a cause of action is surprisingly difficult

Weak cases where there is nominal injury and weak facts about content moderation will be dismissed at as early a stage as if there were immunity. For instance, somebody being called a "b*tch" on Twitter would never succeed with a negligence claim and it would be dismissed at no earlier a stage than the 12(b)(6) motion to dismiss stage used by tech companies presently. Take another example of the often catch-all cause of action but with a very high bar, intentional infliction of emotional distress. The elements of this claim require a plaintiff plead a defendant acted intentionally or recklessly, the defendant's conduct was extreme and outrageous, the defendant's act is the cause of distress, and the plaintiff suffers severe emotional distress as a result. Let's say a politician sues Facebook for intentional infliction of emotional distress for removing a post that encourages violence. Facebook could easily argue that its decision to moderate its content was neither extreme nor outrageous nor that it caused emotional distress, let alone severe emotional distress.

Nothing will be procedurally different for defendants without Section 230 because rarely do they rely on Section 230 alone.

Without Section 230 immunity, nothing would procedurally change for tech companies in getting weak cases dismissed. Tech companies usually make initial (pre-discovery) motions to dismiss based on a variety of grounds, including failure to state a claim, Section 230 immunity, outside the statute of limitations, lack of jurisdiction, First Amendment and anti-SLAPP. In product liability cases, they deny they're a product. Poor cases will be dismissed at this early stage and before the rigors of discovery.[4]

Anti-SLAPP laws are a faster and harsher deterrent for Defendants to get weak and constitutionally protected speech-based claims dismissed.

Plaintiffs bringing frivolous content-based cases like the two described above (negligence claim for being called a bitch on Twitter and IIED claim for a platform removing inciting content) are far more deterred by Anti-SLAPP laws than section 230. Strategic Lawsuits Against Public Participation (SLAPP) provide an accelerated and even profitable way for defendants to get flimsy cases thrown out. Thirty-five states have anti-SLAPP laws. Written into many Anti-SLAPP statutes is a condensed briefing schedule, and the requirement that courts prioritize these cases. Anti-SLAPP statutes create a two-prong test. A defendant must show they're being sued for constitutionally protected speech and then the burden passes to the plaintiff who must show a likelihood of success of winning on the merits of their case. Because Anti-SLAPP motions occur before discovery and it's up to the court's discretion as to whether to allow limited discovery in these motions, plaintiffs are already at a huge disadvantage because the second prong requires a mini trial wherein plaintiffs must provide evidence that they can meet the elements of the cause of action but without the plaintiff having the benefit of discovery. The biggest source of deterrent is the required fee-shifting. A plaintiff who loses their anti-SLAPP motion must pay the defendant's legal and fees. Legal fees typically add up to six figures in Anti-SLAPP motions.

Uninformed plaintiffs sue anyway

Section 230 immunity already does not deter pro se litigants with truly frivolous cases. Folks hellbent on suing will sue with or without the immunity and likely will not even learn of Section 230 immunity until their case is already being dismissed.

Proving psychological injuries is challenging

The majority of cases against big tech involve psychological – and not physical injuries. Proving a psychological injury can be more challenging than a physical one. While there are photographs, x-rays, and courtroom three-dimensional models that aid in proving physical damages, often victims of emotional distress keep the full extent of their injury

[4] See e.g. *Ziencik v Snap* where the plaintiffs alleged the platform breached its duty by failing to report harassers to law enforcement., No. 21-7292, 2023 WL 2638314 (C.D. Cal. Feb. 3, 2023), where the court smartly found no immunity under Section 230 but dismissed the negligence claim for lack of duty, dismissed the Stored Communications Act claim because Snap lacked a "knowing or intentional state of mind," dismissed the consumer protection claims for lack of standing as "consumers," and dismissed the misrepresentation claims because there was no affirmative misrepresentation.

private. The victim is responsible for describing their emotional injury and eliciting empathy from the jurors who may well blame them. Defendants have an easier time sowing doubt in a jury, claiming the victim is at fault or is lying or exaggerating the harm or that earlier or later traumas caused the anguish. Because the claims are far more difficult to prove, lawyers are disincentivized from taking anything but the most egregious cases.

Mandatory arbitration clauses are anti-plaintiff

Many platforms require that their users agree to terms of service that include arbitration clauses. Although enforcement of mandatory arbitration has fallen out of favor and is sometimes unconscionable because of the disparate bargaining power, tech companies do try to enforce these clauses. Arbitration is a deterrent to litigation because it is expensive, favors corporate defendants, and is not public.

Will the ICS really be paying for legal defense or claims itself?

Responsible businesses have liability insurance.

IV. Removing Section 230 immunity will not squash platforms that are little or new

One defense for preserving Section 230 is concern that small or young platforms will not survive. There is no data showing that tech companies are any more or less likely to survive than other businesses. If a small online service provider does fail, it's more likely the result of not being able to compete with the monoliths or obtain the seemingly obligatory venture capital funding.

According to the United States Small Business Administration (SBA), 99.9% of businesses in the United States are small with under 500 employees. There are 33,185,550 small businesses in the US. Small businesses employ 61.7 million Americans, totaling 46.4% of private sector employees. The survival rate of small businesses is 67.7% for two years, 48.9% for five years, 33.7% for ten years, and 25.6% for fifteen.

In all industries, running a small business is difficult. However, all small businesses in this country exist without enjoying immunity from litigation, with the exception of the tiny few that are interactive service providers in the business of publishing third party content. The solution for businesses is to 1) not engage in conduct that harms people, 2) employ the standard of care in your industry, 3) not release unreasonably dangerous or defective products into the stream of commerce, and 4) have liability insurance that protects from financial costs in the face of litigation or judgment.

The "Wikipedia Dilemma" is exaggerated.

The favored example about small sites being jeopardized if Section 230 goes away is Wikipedia, the content-based crowd-sourced encyclopedic platform. The most recent public reporting (June 30, 2023) shows that Wikimedia Foundation, the nonprofit that

supports Wikipedia, is not small or vulnerable. In 2023 it reported assets of $274m. Like all speech-based cases against platforms that host others' content, if sued, Wikipedia has robust defenses such as the first amendment, anti-SLAPP (which would require the plaintiff pay its legal fees), and causation. In other countries where there is no Section 230, Wikipedia has prevailed and not toppled in the process. (See, e.g. Sorin Ceran who sued the administrators of Romanian Wikipedia in Romanian courts claiming "patent falsities", see also the French case where Wikimedia was sued for describing three individuals as gay activists where the court determined Wikipedia found it was not liable because it "did not in fact know of [the content's] illicit nature." What's more, Wikimedia Foundation does not shy away from itself commencing litigation (see e.g. *Wikimedia Foundation, Inc. v. WordLogic Corporation, et al.,* in a patent dispute.)

Of Greater Concern is the Malicious Sites unjustly enriched by Section 230

Some of the internet's most malicious sites are small sites. For decades, the worst offenders of intentional online misconduct have been small sites. Websites that peddled solely in revenge porn and trafficking were emboldened – and even protected by -- Section 230. Nowadays, small websites that solely let people publish digitally enhanced nude images (deepfakes) say they are immune under Section 230. So, too, does a website that glorifies suicide, provides instructions for how to do it, and lets people live-post their suicides.

V. GenAI--The next generation of harm is at our doorstep

The advent of generative AI is guaranteed to bring about unknown harms to individuals and populations. Companies like Snap are already powered by OpenAI's GPT offering children a new feature called "My AI" which they describe as an "experimental friendly chatbot" that can "help and connect you more deeply to the people and things you care about most." The App Store and Google Play have an array of apps that "nudify" images, including those of children. On May 20, 2024, the DOJ announced they arrested a man from Wisconsin who used a text-to-image GenAI product called Stable Diffusion to create thousands of nude images of prepubescent minors "lasciviously displaying or touching their genitals.[5]" He was also caught teaching a fifteen year old how to use the product and direct messaging images to the minor via Instagram.

The risks to children of GenAI tools are beyond the imagination especially as bots become more personal and emotional, where animate and inanimate blur. The risk of influencing child perceptions, inciting behaviors, and causing violence and self-harm are potent. Already Amazon's Alexa challenged a child to electrocute herself by sticking a coin in an electrical socket.[6] And Snapchat's AI chatted with reporters posing as children about booze and sex.[7] With friendly bots, children are apt to disclose deeply personal information which the app can use both for its own commercial purposes, but

[5] United States v Steven Anderegg, W.D. WI, Case No. 24-CR-50-JDP

[6] https://www.cnbc.com/2021/12/29/amazons-alexa-told-a-child-to-do-a-potentially-lethal-challenge.html

[7] https://www.washingtonpost.com/technology/2023/03/14/snapchat-myai/

also provides it with material to blackmail the child or that could be leaked in a data breach.

We can expect that GenAI service providers, if sued, will argue that they are entitled to Section 230 immunity based on being sued as a publisher. While it's obvious that information set forth by the AI is not third party content, they will argue that it was prompted by third party content and thus are entitled to immunity. This is under the but-for theory – i.e. but for third party content, the harm would not have occurred. In the recent Central District of CA *Doe v Grindr,* the court said that the but-for test applies not only to content, but also to harms caused by all "functions, operations, and algorithms" because they are "tools meant to facilitate the communication and content of others." Under this interpretation, GenAI platforms could expect to be immune for all harms their platform causes.

VI. Why KOSA does not solve the problem completely

The Kids Online Safety Act (KOSA), introduced in the Senate, is a response to platforms' to profound evidence showing that platforms sought to addict children and regularly exposed them to harmful content. The blockbuster feature is the imposition of a "duty of care" that requires that platforms "exercise reasonable care in the creation and implementation of any design features to prevent and mitigate" specific "harms to minors" such as mental health disorders, violence, drug use, etc. The law sets forth design features that must be embedded in the app such as privacy settings and the ability for parents to supervise their child's activities. The most recent iteration of the bill has been approved by organizations that typically oppose online regulations, such as free speech and digital rights organizations.

Kosa provides families with the tools, safeguards, and transparency to protect against threats to children's health and well-being online with platforms required to protect children's information, disable addictive product features, and opt-out of algorithmic recommendations. Social media platforms are required to perform an annual independent audit assessing risks to minors, their compliance with KOSA, and whether the platform is taking meaningful steps to mitigate harms. Lastly it allows academic researchers access to critical datasets so they can research harms to the safety and well-being of minors.

While KOSA is laudable for many reasons, it does not solve the problems imposed by Section 230. First off, it does not amend or interplay with Section 230 in any way. The bill does not impact the liability of tech companies at all or provide the children and families it's supposed to protect with any means of enforcement. Instead, only the Federal Trade Commission (FTC) can enforce it. So any child who is harmed because of a tech products failure to comply with KOSA continues to have no right to hold that platform accountable.

In addition to not opening the courthouse doors for the minors it's intended to protect, KOSA provides no protections to people 18+.

VI. Removing Section 230 will not break the internet

For 28 years Section 230 has been a government subsidy for companies, saving them the costs of investing in safety measures for their products and paying for the injuries they've caused. Worse, it's neutered the justice system so that these companies can operate outside the rule of law. The financial pressures typically imposed by consumer safety standards – the threat of being sued if you release unreasonably harmful products into the stream of commerce – is all but nonexistent. Consequently, online companies have no incentive to prevent injuries, intervene when a harm is underway, invest in infrastructures and staffing to moderate harm, or innovate for safer products.

As the Electronic Privacy Information Center stated in its *Amicus Curiae* brief in the *Doe v Grindr* case,

> Perhaps the strongest demonstration that a properly scoped Section 230 will not break the internet is actual experience: [the] court's decisions not to extend Section 230 have not yet shown any signs of breaking the internet. When this Court recognized that online home rental companies must comply with local regulations against brokering rentals for unregistered properties, Homeaway.com, 918 F.3d at 683, it did not cause online rental platforms to fold. When this Court said that app developers still have a duty to design safe products, see Lemmon v. Snap, 995 F.3d 1085, 1092–93 (9th Cir. 2021), platforms did not adopt draconian measures to crack down on user-generated content. When this Court found that websites still have a duty to warn users about known dangers to their safety, see Internet Brands, 824 F.3d at 853, it did not destroy web forums. And when this Court held that social media companies have a duty to abide by content moderation promises they make to users, see Barnes, 570 F.3d at 1109, it did not destroy social media.

Defenders of Section 230 like to say that peeling back immunity would be the "ultimate Pyrrhic victory" and be at the cost of free expression. This overwrought pearl-clutching is not based in reality. The Supreme Court already refused twice in 2023 to not engage in cases with a "complaint that appears to state little, if any, plausible claim for relief." *Gonzalez v. Google (*598 U.S. 617 (2023)) *Taamneh v. Twitter* (598 U.S. 471 (2023)_.

VII. The Fix

Section 230 ought to be sunsetted via the Sunset Clause. However, if Congress fails and instead pursues other legislative avenues, any **legislation must distinguish between hosting defamatory content versus enabling criminal conduct. The first deserves 230, the second does not.**

- Conduct carve-outs
    - Bad Samaritan carve-outs – no immunity from civil liability for platforms that

        - purposefully facilitate or solicit third party content or activity that violates criminal law;
        - Are willfully blind to illicit conduct, (e.g. failure to detect or respond to illegal conduct, preventing or seriously inhibiting swift detection and banning of offenders, impeding law enforcement's ability to investigate and prosecute serious crimes, and depriving victims of the evidence they need to bring civil claims against their perpetrator)
    - Egregious conduct carve-outs – no immunity for the worst type of conduct -- claims involving child exploitation, sexual abuse, terrorism, and stalking. Section 230 was never intended to shield platforms from liability so far outside the original purpose of the statute
    - Actual knowledge and court judgments – no immunity where a platform has actual knowledge or notice that the third party content violates criminal law or ignores a court order indicating that content is unlawful or that published content or conduct on a platform underlies a criminal case or civil restraining order.
- Injunctive relief to help in emergency cases where the plaintiff is suffering imminent harm because of harms on a platform or a court has ruled content unlawful or when the basis of a criminal case or civil restraining order is content or conduct occurring on a platform
- The ICS is the ICP and therefore not entitled to immunity for claims pertaining to
    - Breaches of its own terms of services;
    - Breached promises made to users or the public;
    - Testimony of its executives under oath;
    - Constructive notice of the specific harm and damages; or
    - Paid content, including in-kind payment. This includes payment to or from the ICS;
    - Content recommended to users via algorithm;
    - Defectively designed or manufactured products or failure to warn;
- Define "information content" to include only speech-based content
- Limit immunity to only publication-related torts like defamation.
- Clarify that generative AI is the platform's own content

VIII. Conclusion

What is illegal online, should be illegal offline. Americans are being injured by tech companies running amuck, unconstrained by regulation, liability for their product, or the threat of litigation. Everyday people lost their fundamental right to the courts to vindicate their injuries. This has created an undeserved windfall for the tech industry, allowing it to become the most powerful, wealthy, omnipotent, and omniscient industry in the history of the world. The trio of corporations, courts, and Congress birthed a monster. Through legislative reform, Congress can fix what corporations won't because of greed and court's can't because of bad accumulated case law. Anybody could become my next client.