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

"Holding Big Tech Accountable: Targeted Reforms to Tech's Legal Immunity"

December 1, 2021

Chair Doyle, Ranking Member Latta 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platforms and the heartbreak of trying to get justice for my clients but being locked out of our courts because of an outdated law, Section 230 of the Communications Decency Act.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 -- 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*.

This testimony looks at three of my cases, each in different phases of litigation, impacted by the culpable tech companies' claim of immunity, provides some historic context, laments the overreach of our courts in interpretating Section 230, explains why reforming the law will not cause a stampede of litigants to the courts, looks at the four bills being discussed today, and presents a summary and redline of what needs to happen in Section 230 reform to protect the most serious victims and deter the worst of tech's antisocial business practices. My proposal takes bits and pieces from the four proposed bills, as well as recommendations from the Department of Justice's 2020 Symposium about Section 230.

In summary, we must:

1. **Remove immunity for Bad Samaritan platforms that purposefully facilitate or solicit criminal conduct or are willfully blind to it;**

2. **Create carve-outs for the most seriously heinous conduct such as child sexual exploitation, terrorism and cyber-stalking and the most serious types of injuries like wrongful death; and**
3. **Eliminate immunity when platforms have actual knowledge of injurious conduct or ignore a court order.**

I. Intro

I've been vindicating the rights of severely traumatized people since graduating college in 1999. I began my career as a case worker for Nazi Victims and Holocaust Survivors in New York City, providing this dwindling and important group with social services and applying for the various new reparations that materialized in the early 2000's. Suddenly Germany's social security system recognized forced ghetto labor as pensionable. Swiss banks were aggregating lists of dormant accounts from the 1930's and 1940's which were made available on the internet. And there was a new one-shot payment of $2500 for living survivors of concentration camp medical experiments. I was engrossed with the crudeness of assigning money to suffering and how rarely it measured up to the suffering it attached to. I enrolled in law school in the evening, continuing with my Survivors in the daytime. When I graduated with my JD I went on to work at the Vera Institute of Justice where I sued individuals and companies who'd exploited vulnerable people who'd been deemed incapacitated.

In 2014, after narrowly surviving a trauma related to a dangerous individual I met on a dating app, I left my job at Vera and started my law firm to represent victims of online harassment, sexual assault, and personal injuries against big tech. The work was personal and I set out to get restitution and reparations for severe injuries and fatalities to my clients caused in the most modern of war zones, the internet.

Money does not undo injuries or erase traumas. But court's reallocation of money from the injurer to the injured is the best method of justice we have for improving life for victims and deterring future bad acts of offenders. I learned two very important things from the Holocaust Survivors which guide my work at the firm: 1) if somebody hurt you, somebody must pay 2) the only way to stop history from repeating itself is to bear witness and tell the story over and over again until change comes about. That's what I'm here to do today.

I'm one of just a handful of lawyers in the country who litigates against technology companies on behalf of users who've been catastrophically hurt. Section 230 of the Communications Decency Act, that aforementioned law from the 90's, makes it virtually impossible for plaintiffs wounded by tech companies to get beyond the front doors of the court before their case gets tossed to the curb like garbage.

* * * * *

K.M., a client story
Stage: Pre-litigation

Let me tell you about a Zoom conversation I had with one of my clients and her mother on Friday. K.M. looks sheepish when I ask how she is. She says good and gives her mom the side-eye. Oh, and she hates her new school she just switched to. I tell her I like her new necklace and earrings. After K.M. leaves her bedroom, her mom tells me that K.M. was hospitalized again, this time with fifty pills of Benadryl in her belly. It's her third attempt since I met her in May of 2020. This time it's because an eighteen year old boy said he wanted to hit her after he got in trouble for kissing her at school. Last time it was after confiding that she performed oral sex for somebody on the bus. I ask K.M.'s mom if all this behavior is related to the online exploitation. She says yes, the therapist believes K.M.'s inability to measure sexual risk stemmed directly from that and K.M. was never the same after.

The "that" began in April 2020 when K.M. was 11 years old. She was stuck at home during the most dire stage of New York City's Coronavirus lockdown and met a guy on Instagram who shared her interest in Japanese animè. The guy got K.M. to send him pictures and tell him secrets. Before long, he was coercing and blackmailing her into sending him pictures and videos, dozens of them, of her naked body, masturbating, and inserting objects into her vagina. K.M. would stay up all night in the bathroom, so she wouldn't wake her sister, doing what he wanted. The offender direct messaged K.M. about obscene things, making her agree to plans of incest and gangbangs on their future children. Using all this material, the offender coerced K.M. into sharing the passwords to her Instagram accounts. After not sending him the 150 nudes he demanded one night, the offender attempted to post nude images of K.M. publicly onto her Instagram Story. Locked out of her account and unable to stop him, K.M. received a notification on her phone saying images were blocked from being posted on her Story because of inappropriateness. Instagram seemingly identified nude images coming from a child's account and prevented them from being posted. The offender shifted gears and began distributing the images from K.M.'s account to K.M.'s followers by direct message. Instagram did not block the image when disseminated through direct message, despite earlier saying it knew it was a child's account. K.M.'s account sent it to sixteen people, fifteen of whom K.M. knew personally, and twelve of whom were young teenagers. When K.M.'s aunt told her sister (K.M.'s mom) she'd received these images of K.M., K.M.'s mom immediately tried to find the phone number for Instagram. She went on the website and frantically googled the company, but couldn't find a phone number or email address. K.M.'s mom, an immigrant from Guatemala who cleaned houses for a living did not herself have an Instagram account. Her daughter remained locked out of the account. The guy still had control. Desperate, K.M.'s mom took her to the police precinct where the reporting officer lectured them that they ought to learn the difference between "discipline and crime" before sending them on their way.

K.M. was forced to transfer schools because she was too humiliated to even be in Zoom class with the other kids. K.M. was unable to cope with the shame. She suffers from extreme guilt for putting her family through this experience. She says she feels like everybody thinks she's disgusting and that she's ruined her family. Her father moved out of the house and their dog died one after the other. She began cutting herself and says she feels dead at times. At some point, either after the first or second hospitalization for suicide attempt, child protective services opened a negligence case against K.M.'s mom for leaving her daughter unattended for short spurts while she cleaned houses. This will be on her permanent record until K.M. is 28 years old and will impact her immigration status. K.M.'s mom is down to three half-day cleaning shifts a week and was forced to put the family on welfare. She could go to jail if she is caught leaving K.M. alone again. They can't afford to live.

* * * * *

I've not yet brought claims for K.M. Litigation would be too stressful for her at this point and could lead to another suicide attempt. An attempt, or worse. Facebook/Instagram (sorry, I refer to indulge their rebrand or buy into a new dimension they are putting a stake in) make a show of advertising online and on television that they want reform and regulation. However, it's smoke and mirrors. In reality, they still parade around saying they are immune from liability both in litigation and pre-litigation settlements because of Section 230 and refuse all responsibilities for injuries they cause to people like K.M. When I think of Section 230 reform, it's through the litmus test of whether it will vindicate K.M.

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 a broader bill intended to combat pornography on the internet which lawmakers realized children were accessing. 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 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 coldshoulder 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 past 25 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 obscenity, 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 and obscenity, 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.

* * * * *

Matthew Herrick: A client story
Stage: Post-litigation

It all started one evening in late October 2016, right before Halloween. Matthew sits on the front stoop of his New York City apartment, smoking a cigarette, when a stranger calls to him from the sidewalk and starts heading up the steps toward him. The stranger's tone is friendly and familiar. But Matthew has never met this guy before. "I'm sorry," he says. "Do I know you?"
The stranger raises his eyebrows and pulled his phone from his back pocket. "You were just texting to me, dude," he replies, holding out his phone for Matthew to see. On the screen is a profile from the gay dating app Grindr, featuring a shirtless photo of Matthew standing in his kitchen, smiling broadly.

The stranger keeps holding up his phone, insisting Matthew had invited him over for sex. But Matthew knows the profile isn't his. Finally, the stranger becomes exasperated and leaves. "Fucking liar!" he shouts in Matthew's direction as he walks away. "You're an asshole!"
Rattled, Matthew goes back inside. A few minutes later, he hears his buzzer ring. It's another man insisting that he, too, had made a sex date with Matthew. Two more men show up that day. And three others came calling the next. "Matt!" they holler from the sidewalk, or they'd lean on the buzzer expecting to be let in. At first the strangers only go to his apartment, but by the end of the week a steady stream of men are showing up at the restaurant where Matthew works as well. Some in their 20s, others much older. A few arrive in business suits, as though on the way to the office. Others are twitchy and sweaty, looking like they'd been up all night getting high. They'd stalk him at work and at home, all hours of the day and night, each one convinced Matthew had invited him over for sex.

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. Like many of my clients, before coming to see me 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. The officers dutifully took down his information but didn't seem to understand the danger he was in.

By the time Matthew came to me for help, the Manhattan district attorney opened an investigation and he'd gotten a family court "stay away" order, but neither was stopping the traffic of strangers coming to his home and work for sex. He also did everything he could to get the imposter profiles taken down. He directly contacted Grindr and its competitor Scruff, which Matthew's ex was also using to impersonate him. In their terms of service, both companies explicitly prohibit the use of their products to impersonate, stalk, harass or threaten. Scruff, the smaller of the two companies, responded to Matthew immediately. It sent him a personal email expressing concern, took down the fake accounts, and blocked the ex's IP address, effectively banning him from the app. When the ex started impersonating Matthew on Jack'd, yet another gay dating app, that company also banned him from using its platform to harass Matthew. But Grindr took a different approach: It did absolutely nothing.

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, as many as 23 in a day, arrived in person at Matthew's home and job.

Grindr is a wildly successful company. In 2018, the dating app reportedly had more than three million users in 234 countries. Like most social media companies, Grindr operates, in large part, as an advertising platform. The free content and services these platforms provide—porn, photo sharing, direct messaging, emailing, shopping, news, dating—are really just lures to get people

to show up so the companies can collect data about what users buy, who they're friends with and where they're going, and use that information to advertise. Grindr prides itself on its state-of-the-art geolocative feature, which can pinpoint a user's exact location, allowing users to match with others in their vicinity. This is how they rake in advertising revenue—by customizing the ads that users see based on nearby businesses.

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.

I didn't need to explain on a technical level how Grindr was being used against Matthew at this stage of the litigation; that's what discovery is for. What we knew is that Grindr was in an exclusive role to help stop Matthew's hell, given law enforcement was too slow and the ex had been deterred by neither arrests nor orders of protection.

I knew from the start that Grindr would claim it was immune from liability pursuant to Section 230 of the Communications Decency Act, which states that "[n]o 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."

So I made sure not to sue Grindr for traditional publication torts like defamation. That is, I was not suing them for any words the ex said on the profiles or communications he'd made on the app. Instead, I tried something new—I sued Grindr using traditional product liability torts. I argued that 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.

On Feb. 8, 2017, Grindr filed a notice of removal from state court to the Southern District of New York. Our temporary restraining order requiring that Grindr ban the ex from its services expired as a matter of law 14 days after the removal—but when we moved to extend the order, Judge Valerie Caproni denied the extension. Judge Caproni felt our underlying case lacked merit because she suspected Grindr was immune from liability pursuant to the Communications Decency Act, arguing that 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. In April and May of 2017, Grindr and its holding companies filed motions to dismiss our claims. At the time, Matthew's ex was continuing to relentlessly use the app to send strangers to his home and job—a fact the court knew.

We argued in our opposition papers 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.

Nevertheless, on Jan. 25, 2018 Judge Caproni dismissed our complaint entirely. All but a copyright claim was dismissed with prejudice, meaning that even if Matthew learned new information to support his claims, he could not amend his complaint.

Matthew's case was thrown out before we'd even gotten our foot in the door—even though dismissal at the motion to dismiss stage is supposed to be reserved for situations where a complaint is defective on its face, while ours was a detailed, thorough 43 pages and well-pleaded. The judge relied on Grindr's immunity under Section 230.

To our disappointment, 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, also was denied. It was the end of the road for *Herrick v Grindr*.

* * * * *

The Supreme Court has never ruled on the proper scope of Section 230. As Matthew's case demonstrates, this is a matter of life or death for victims of stalking and violence caused and exacerbated by computer technologies unimagined when Congress passed the law in 1996. Decades ago, lawmakers had this pie-in-the-sky idea that internet companies would monitor content their users uploaded to protect the rest of us. What's become painfully apparent, and arguably should have been obvious, is that without the threat of legal liability hanging over their heads, companies like Grindr really don't care about who gets hurt.

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."

Fortunately, our product liability theory has been advancing places outside the 2nd Circuit. In 2021's *Lemmon v Snap*, the 9th Circuit said Snap was not immune from liability for one of its features, an app filter which the court said encouraged kids to drive fast. Consequently, the plaintiffs may move forward with their theory of liability that the feature contributed to the deaths of the young men using the filter and crashed their car at 120 mph.

III. The Court's Too Broad Interpretations of Section 230

Joining Herrick v Grindr in the court's broadening interpretation of section 230 are the following:

- *Dyroff v. Ultimate Software Group, Inc.*, 934 F.3d 1093 (9th Cir. 2019), the Court held that there was no material contribution when a website connected two users to each other based on the free- form comments they wrote on the site about their interest in heroin. A teenager died of fentanyl poisoning after the other user sold him fentanyl instead of heroin.

- *Force v. Facebook, Inc.*, 934 F.3d 53 (2d Cir. 2020), the Court held that Facebook did not materially contribute to illegal content where its algorithm amplified terrorist content. Arranging and displaying third party user's content to others was not material contribution.

- *Jane Doe No. 1 v. Backpage.com LLC*, 817 F.3d 12 (1st Cir. 2017). There, sex-trafficking victims sued Backpage.com, a classifieds hub that (among other things) hosts online advertising for illegal commercial sex in the United States. Even though the plaintiffs had marshaled persuasive evidence that Backpage.com had adopted rules and practices that facilitated sex trafficking—from selectively removing postings discouraging sex trafficking and tailoring its rules to protect sex trafficking from detection to removing metadata on photographs—the First Circuit concluded that Backpage was entitled to Section 230 immunity. This led to a Congressional amendment.

- *Goddard v. Google, Inc.,* 640 F. Supp. 2d 1193, 1196 (N.D. Cal. 2009). There, the plaintiffs alleged that Google's Keyword Tool suggested words to include in advertisers' ads and often added words that resulted in false advertisements (such as turning the word "free" into "free ringtone" even though the advertised service would not be free). But the district court concluded that the Keyword Tool was a "neutral tool" that had immunity—even though Google had itself suggested the false phrases that advertisers had used in their ads

- *Fields v. Twitter, Inc.,* 217 F. Supp. 3d 1116 (N.D. Cal. 2016). There, the plaintiffs argued that Twitter's provision of accounts—which ISIS members then used to communicate with one another, recruit members, and spread propaganda—amounted to providing material support for terrorism. See id. at 1119. But the district court found Twitter categorically immune under Section 230. According to the court, giving ISIS members Twitter accounts was "publishing activity" for Section 230(c)(1) purposes because handing out accounts necessarily "include[s] decisions about what third-party content may be posted online."

IV. 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 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. In this section I discuss why we need not fear a stampede to the courthouse.

The onus is on the plaintiff to prove liability.

Like all litigation, the onus is on the plaintiff to *prove* the merits of the case and the plaintiff will sometimes fail. 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.

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. Rare is the client with millions of dollars to fund cases against tech. 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. My tiny firm spent over a million dollars of lawyer time losing Matthew's case. Consequently, frivolous and low injury cases are eliminated before they're ever filed.

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 "bitch" 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, and anti-SLAPP. Poor cases will be dismissed at this early stage and before the rigors of discovery.

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 contet) 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 four 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.

The two examples discussed above – the negligence case based on rude behavior and the IIED case about a moderation decision – if brought against an Interactive Computer Service (ICS) would both most certainly be dismissed in an Anti-SLAPP motion and the plaintiff could expect to be forced to pay punishing legal fees for both their own attorney and the defendant's.

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 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.

Will the ICS really be paying for claims itself?

All responsible businesses have liability insurance. It would be shocking if a user-facing platform did not have an insurance policy to deal with lawsuits. I suspect the biggest impact of removing Section 230 immunity will play out in the world of insurance.

* * * * *

A.M: A client story
Stage: In litigation, filed November 19, 2021

He is 37.
She is 11.
They both are on the site Omegle.
The banner up top says "talk to strangers."
Omegle matches the two to video chat.
The man comforts her in her 11 yo loneliness.
At first he wants to see her smile.
Then he asks her to show another body part.
And another *and another* .
She does protest. And he says you're free to stop. But alas, I'd have no choice but to send these videos to your parents and friends at school. And the police. You don't want to get in trouble do you? You've created child pornography and will go to jail.
This goes on for 3 years.
He makes her perform for he and his friends. He forces her to recruit more kids on Omegle.
One day an FBI agent contacts A.M.'s parents. They say they tracked them down after Canadian police did a raid on a man's home, a home he shared with his wife's daycare business. And they discovered 3000 files of porn, including several hundred of a young girl. In one, that young girl is wearing a sweatshirt with the name of the same school A.M. attends. The school recognized her as A.M.
Just like that, her nightmare ended. Except it didn't. Ever since, A.M. suffered extreme social anxiety, panic attacks, and breakdowns. She was still convinced that he would kidnap her or have her arrested. At first, she'd wanted to go to his aid.

* * * * *

We filed A.M.'s lawsuit against Omegle ten days ago. The media was full of stories of children being preyed upon by predators on this platform, including one BBC article where the journalists went undercover and were astonished by the number of both

masturbating children and adults they were randomly matched with, it being apparent that adults were there for one extremely disturbing purpose. Like in Matthew's case, the heart of the claims is that it was a defective product in that it is clearly used by children and adults for sex videochatting, yet does nothing to separate the two populations. Judging by its track record, Omegle will say it's her fault and that it says right there on its site that it's for kids 13 and older, as if the outcome would have been any different if she'd been two years older. Omegle will say they are free to pair adults and children and have no duty to prevent abusers, that Section 230 protects them from lawsuits like this.

V. The four reform proposals on the table today

The four proposed bills discussed at today's hearing are a step in the right direction toward correcting the overbreadth our courts interpreted into Section 230. Each of them contains laudable elements.

The Civil Rights Modernization Act of 2021 (H.R. 3184) removes the liability exemption for targeted ads that discriminate. This is important because companies should not be immune from liability for content like ads they profit from. I'd take it steps further, in my opinion, the monetization of content ought to transform the Interactive Computer Service into an Information Content Provider with relation to said content. Alternatively, with paid content, the platform is not truly performing the role of an Interactive Computer Service, but rather the role of a billboard or marketer. Narrowing the definition of ICSs and ICPs accordingly to address when paid content transforms these designations is a more expansive way to address the issue. Lastly the CRMA only applies to claims pertaining to injuries stemming from civil rights violations. Unfortunately, this would exclude the most vicious harms and serious injuries we see online which are not typically based on discrimination, but violence.

The Protecting Americans from Dangerous Algorithms (H.R. 2154) smartly and appropriately classifies algorithms as ICP. This law is so narrow as to be almost unusable. It excludes so many presentations of algorithms (i.e. ranked, ordered, promoted, recommended, amplified, or altered in a way that is obvious, understandable and transparent to a reasonable user, chronologically listed, sorted by user ratings or numbers of reviews, alphabetical, random, organized by views, downloads or similar.). It applies only to large companies which is a disappointing delimiter since some of the most deliberately malicious platforms are small. Oddly, it rules out all claims except those pertaining to equal rights and injuries from international terrorism. My clients would stand no benefit.

The Justice Against Malicious Algorithms Act (H.R. 5596) is a far superior way to address injuries caused by algorithms than H.R. 2154. This bill creates a new exception to immunity for suits against ICS' for injuries caused from algorithmically directing a user to material that causes them injury. I could envision this applying to scenarios exposed recently such as Instagram directing teen age girls to thinspiration and weightloss content and playing a causal role in the eating disorders that result. I further envision this benefitting my clients who are matched through dating apps with dangerous individuals, such as my client, Matthew Herrick. I do fear that the exception

to the exception for user-specified searches will create a sinkhole many worthy plaintiffs will fall into. I also recommend against the narrowing mens rea requiring the ICS "knew or should have known" or "acted recklessly." These will be abused by defendants an overinterpreted by courts. Lastly, injuries ought not be limited to "physical or severe emotional injury." Although most of my clients do suffer severe emotional injury, we must not overlook financial injuries and the like.

The Safeguarding Against Fraud, Exploitation, Threats, Extremism, and Consumer Harms Act ("SAFE TECH Act**")** (H.R. 3421), of the four bills, this one will vindicate the injuries I deal with the most. First, in (c)(1) it changes the immunity from applying to "any information" provided by a third party to "any speech" provided by a third party. Hopefully courts will recognize this as an attempt to for courts to start distinguishing between content (immune) and conduct-based (hopefully not immune) harms.

SAFE TECH also removes immunity for speech that the ICS profited from or funded. As I have long advocated, this bill requires that 230 immunity be an affirmative defense for which the defendant has the burden of persuasion. This has the advantage of unburdening the court with having to play computer scientist in a 12(b)(6) decision, determining without facts from the defendant that they are in fact an ICS being treated as the publisher or speaker of information provided by another ICP. Other excellent provisions of SAFETECH include the immunity exclusion for injunctive relief which is important when a victims' main concern is getting illegal material such as nonconsensual pornography or child sexual exploitation material off the web site. Finally, it creates five new categories of carve-outs: claims relating to 1) civil rights laws, 2) antitrust laws, 3) stalking, harassment or intimidation laws, 4) international human rights laws, and 5) wrongful death actions.

The carve-outs are good, especially in that they apply to both state and federal laws but require some tweaking of the language in order to be useable by injured plaintiffs in litigation. Most specifically we need the carve-outs to apply to the facts and not laws. A technical point, but an important one. Many crimes, such as stalking, harassment, human rights abuses, do not have a private right of action. That is, victims can't sue for the violation of these laws, but rather must use classic tort law to make their claim. For instance, my stalking clients in New York could not bring a lawsuit against their stalker or a platform that facilitated the stalking because there is no private right of action for stalking. Stalking is only a criminal law. Instead, a victim would sue the platform for negligence or breach of contract or negligent infliction of emotional distress. We also must eliminate the delimiter on the stalking, harassment and intimidation carve-out which requires "in whole or in part" that the harmful conduct be based on a protected class (i.e. sex (including sexual orientation and gender identity), race, color, religion, ancestry, national origin, physical or mental disability")

VI. Carrie's fix

We have a real mess here, but a fixable one. Congress created Section 230 and has the power to fix it. Any proposals for reform I consider through the lens of the most wrenching harms I see in my office. **Any legislation must distinguish between**

hosting defamatory content versus enabling criminal conduct. The first deserves 230, the second does not. In addition to the three clients I described in detail here (K.M., Matthew Herrick, and A.M.) here, reform must provide paths to justice for the following clients, a small sample of our cases, who've suffered devastating injuries:

- The family of a 27-year-old man who was directed to Amazon.com from a pro-suicide website and sold sodium nitrite, delivered by Amazon Prime, he killed himself two days later. In the middle of the suicide, he indicated he didn't want to die but it was too late. Amazon removed user reviews, manipulates the star rating, refused to put known warnings on the bottle or its website which should have contained an effective way to reverse the effects (methylene-blue), and strategically cropped photos of the product against its own terms of service to exclude the warning label. We've spoken to four other families who lost a loved one from Sodium Nitrite purchased on Amazon.
- The families of seven children who were each sold one fentanyl-laced pill on Snap. All died. The youngest child was 14, a skateboarding phenom. Snap has refused to crackdown on the Fentanyl murders it's facilitating despite the United States hitting its all time record for drug overdoses in 2020, largely because of Fentanyl.
- The family of Bianca Devins whose murder was liveposted on Instagram. Instagram facilitated the spread of her murder images by refusing to remove the murderer's account. Its explanation? They said they needed confirmation the account did not instead belong to somebody impersonating the murderer. To date, Instagram refuses to give Bianca's family control over her account despite acknowledging it's an asset of the estate. Her family is consistently harassed online and taunted with murder images of Bianca, which Instagram is seemingly unable to hash and remove. Recently, somebody sent Bianca's mom a murder image of Bianca covered in ejaculate.
- The family of Alison Parker, a beautiful and young newscaster who was shot dead on the air. YouTube is unable or unwilling to get the content removed from its platform and the news corporation refuses to transfer copyright of the footage to the family so they can sue YouTube/Google for infringing its copyright (one of the few causes of action the drafters did create an immunity exception for in 1995)
- The young woman who was barely eighteen when she was coerced into filming a very graphic pornography video with three men double her age. After a painstaking negotiation, she purchased copyright from the offenders, but websites, including Google refuse to honor her content removal requests which comply with the Digital Millenium Copyright Act. Unfortunately, a copyright suit will create more attention to the content in question and Google which continues to rank the images high in her search engine results, should be liable not just for intellectual property violations, but for its algorithmic negligence.

Short of eradicating Section 230 my recommendations are most similar to the Key Takeaways and Recommendations published by the Department of Justice in June 2020 after its February 2020 symposium "Section 230 – Nurturing Innovation or Fostering Unaccountability." I was relieved to see many of my own recommendations from that

event adopted by DOJ. These recommendations recognize that large tech platforms are no longer nascent or fragile, if ever they were, preserves competition, and keeps core immunity for defamation to foster free speech.

- 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 obscenity and defamation.

For a full redline version of my proposed reform, the Herrick Act Against Violence Online ("HAAVO"), please see Exhibit A.

VII. 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.

EXHIBIT A

A BILL

To amend Section 230 of the Communications Act of 1934 to reaffirm victims' rights and consumer protections.

SHORT TITLE

This Act may be cited as the Herrick Act Against Violence Online ("HAAVO")

(c) PROTECTION FOR "GOOD SAMARITAN" BLOCKING AND SCREENING OF OFFENSIVE MATERIAL.

(1) TREATMENT OF PUBLISHER OR SPEAKER. (A) No provider or user of an interactive computer service shall be treated as the publisher or speaker of any ~~information~~ speech provided by another ~~information~~ speech content provider.

(2) CIVIL LIABILITY. No provider or user of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, promoting terrorism or violent extremism, harassing, promoting self-harm, or unlawful, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in Subparagraph (1).

(d) EXCLUSION FROM "GOOD SAMARITAN" IMMUNITY.

(1) "BAD SAMARITAN" CARVE-OUT. Subsection (c)(1) shall not apply in any criminal prosecution under State law or any State or Federal civil action brought against an interactive computer service provider if, at the time of the facts giving rise to the prosecution or action, the service provider acted purposefully with the conscious object to promote, solicit, or facilitate material or activity by another content provider that the service provider knew or had reason to believe would violate Federal criminal law, if knowingly disseminated or engaged in.

(2) CARVE-OUT FOR ACTUAL NOTICE OF FEDERAL CRIMINAL MATERIAL. Subsection (c)(1) shall not apply in a criminal prosecution under State law or any state or Federal civil action brought against an interactive computer service provider if—

(A) such prosecution or action arises out of a specific instance of material or activity on the service that would, if knowingly disseminated or engaged in, violate Federal criminal law;
(B) the provider had actual notice of that material's or activity's presence on the service and its illegality; and
(C) the provider failed to do any of the following:
(i) expeditiously remove, restrict access to or availability of, or prevent dissemination of the specific instance of material and take reasonable steps to remove, restrict access to or availability of, or prevent dissemination of the material across the service;
(ii) thereafter report the material or activity to law enforcement when required by law or as otherwise necessary to prevent imminent harm; or
(iii) preserve evidence related to the material or activity for at least 1 year.

(3) JUDICIAL-DECISION CARVE-OUT. Subsections (c)(1) and (2) shall not apply in any criminal prosecution or civil action or injunction arising from the failure of an interactive computer service provider to remove, restrict access or availability to, or prevent dissemination of material within a reasonable time after receiving notice of a final judgment from a court in the United States indicating that such material or activity is defamatory under state law or unlawful in any respect. However, no interactive computer service provider shall be held liable for removing, restricting access to, or preventing dissemination of material in response to receiving such notice.

(4) NOTICE MECHANISM REQUIREMENT. An interactive computer service provider shall make available to the public, without expense, an easily accessible and apparent mechanism for notifying the provider of defamatory or unlawful material or activity as described in Subsections (d)(2) and (3). An interactive computer service provider shall not be entitled to assert immunity under Subsection (c)(1) if it designs or operates its service to avoid receiving actual notice of Federal criminal material on its service or the ability to comply with the requirements under Subsection (d)(2)(C).

~~(d)~~ (e) OBLIGATIONS OF INTERACTIVE COMPUTER SERVICE. A provider of interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.

~~(e)~~ (f) EFFECT ON OTHER LAWS.

(1) NO EFFECT ON CRIMINAL LAW OR FEDERAL CIVIL ENFORCEMENT. Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this Act, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, United States Code, or any other Federal criminal statute. Nothing in this section shall be

construed to prevent, impair, or limit the enforcement by the United States, or any agency thereof, of any civil Federal statute or regulation.

(2) NO EFFECT ON INTELLECTUAL PROPERTY LAW. Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

(3) STATE LAW. Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought, and no liability may be imposed, under any state or local law that is inconsistent with this section.

(4) NO EFFECT ON COMMUNICATIONS PRIVACY LAW. Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986, or any of the amendments made by such Act, or any similar State law.

(5) NO EFFECT ON SEX TRAFFICKING LAW. Nothing in this section (other than subsection (c)(2)(A)) shall be construed to impair or limit—

(A) any claim in a civil action brought under section 1595 of title 18, United States Code, if the conduct underlying the claim constitutes a violation of section 1591 of that title;

(B) any charge in a criminal prosecution brought under State law if the conduct underlying the charge would constitute a violation of section 1591 of title 18, United States Code; or

(C) any charge in a criminal prosecution brought under State law if the conduct underlying the charge would constitute a violation of section 2421A of title 18, United States Code, and promotion or facilitation of prostitution is illegal in the jurisdiction where the defendant's promotion or facilitation of prostitution was targeted.

(6) NO EFFECT ON ANTI-TERRORISM CLAIMS. Nothing in this section shall be construed to prevent, impair, or limit any claim in a civil action brought under section 2333 of title 18, United States Code.

(7) NO EFFECT ON CHILD SEX ABUSE OR CHILD SEXUAL EXPLOITATION CLAIMS. Nothing in this section shall be construed to prevent, impair, or limit any civil action brought under state or federal law relating to claims of child sexual abuse or child sexual exploitation.

(8) NO EFFECT ON CYBER-STALKING LAWS. Nothing in this section (other than 12 subsection (c)(2)(A)) shall be construed to prevent, impair, or limit any civil action in state or federal court relating to harm suffered from conduct that would constitute a violation of section 2261A(2) of title 18, United States Code.

(9) NO EFFECT ON ANTITRUST LAWS. Nothing in this section shall be construed to prevent, impair, or limit any civil action brought under the Federal antitrust laws.

(10) NO EFFECT ON PRODUCT LIABILITY CLAIMS. Nothing in this section shall be construed to prevent, impair, or limit any civil action brought against an Interactive Computer Service for its own defects in its design, manufacture, or failures to warn users and the public of serious risks.

(11) NO EFFECT ON WRONGUL DEATH ACTIONS. – Nothing in this section shall be construed to prevent, impair, or limit any civil action for a wrongful death.

~~(f)~~ (g) DEFINITIONS. As used in this section:

(1) INTERNET.

The term “Internet” means the international computer network of both Federal and non-Federal interoperable packet switched data networks.

(2) INTERACTIVE COMPUTER SERVICE.

The term “interactive computer service” means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

(3) ~~INFORMATION~~ SPEECH CONTENT PROVIDER.

The term “~~information~~ speech content provider” means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service. Being responsible in whole or in part for the creation or development of speech includes, but is not limited to, instances in which a person or entity solicits, comments upon, receives payment or payment in-kind for, funds, algorithmically directs, provides testimony under oath as an executives employed by the interactive computer service, or affirmatively and substantively contributes to, modifies, or alters speech provided by another person or entity.

(4) ACCESS SOFTWARE PROVIDER.

The term “access software provider” means a provider of software (including client or server software), or enabling tools that do any one or more of the following:

(A) filter, screen, allow, or disallow content;

(B) pick, choose, analyze, or digest content; or

(C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.