Section 230 in 2022: The Increasing Responsibility of Online Platform Hosts to Address Human Trafficking and Child Exploitation

Jill Steinberg & Kelly McGlynn[*]

Table of Contents

Abstract

In 1996, before the widespread public use of the internet, Congress recognized the need to regulate improper content online while also encouraging the growth of the then-nascent industry. From these competing values emerged Section 230 of the Communications Decency Act. Now there is an increasing movement in Congress and among the judiciary to strike a different balance. Section 230 has been interpreted to protect entities that host platforms online from liability for the harms that are perpetrated on and allegedly facilitated by their platforms. Among those harms are human trafficking and child exploitation. Wrongdoers are known to use interactive platforms to identify, connect with, and exploit victims. Recent cases show that some courts are no longer inclined to allow Section 230 to fully shield platform hosts from liability. These cases have begun to shift responsibility onto hosts, suggesting that they have some obligation to protect their users from these harms. Section 230 has also been the subject of high-profile political discussion, with demonstrated bipartisan interest in legislative change. This article provides an overview of Section 230 as it stands today, and reviews the cases and legislative proposals that together demonstrate that the law's broad liability shield is already shrinking and may undergo dramatic change in the near future. We discuss the implications this has for entities operating online and conclude that while Section 230 still protects them in some instances as it relates to trafficking and child exploitation material, this may soon change and should spur proactive efforts to implement appropriate safeguards.

[*] Jill Steinberg is a partner at Ballard Spahr LLP in the White Collar Defense and Internal Investigations group, and is a former state and federal prosecutor. Kelly McGlynn is an associate at Ballard Spahr LLP in the White Collar Defense and Internal Investigations group. The views expressed in this article are those of the authors and do not represent the views of Ballard Spahr LLP.

1. **Introduction**

One unfortunate truth about the internet is that every platform that connects people for legitimate and worthy purposes can also be used by bad actors to commit crimes against the vulnerable. Online environments are and have been used to promote sex and labor trafficking and child exploitation. Some entities operating in this space have advanced the position that they are not responsible for content posted by third parties and have relied on statutory immunity when victims of exploitation and trafficking sue them for harms that took place on or arguably were facilitated by their platforms.[1] But now the idea that platforms are not responsible for these users' communications, and that statutory immunity, are being challenged. Immunity is almost certain to shrink. It may even disappear entirely with respect to certain types of claims. Companies operating interactive online platforms should carefully evaluate the existence of and potential for trafficking and child exploitation, and take steps now to address those risks – before these changes make them further susceptible to legal and reputational damage.

This article discusses the role that online platforms play in the growth of – and the fight against –trafficking and child exploitation online.[2] These crimes can be facilitated by any platform that connects people. Platforms where users build relationships also create opportunities for traffickers to find victims, gain their trust, and eventually exploit them. This can happen on dating applications where a user who feels comfortable with a match sends a sexual image, which the match then uses to blackmail and coerce the victim. It can happen on widely used social media sites whose algorithmic suggestions of followers and friends might learn the preferences of a predator and

[1] *See, e.g.*, Doe v. Myspace, 528 F.3d 413, 419-20 (5th Cir. 2008) (applying statutory immunity to bar claims that defendant could have taken steps to prevent a predator from connecting with the minor plaintiff on its platform).

[2] There are a number of terms to refer to these entities, including interactive service providers, platform hosts, companies operating web-based platforms, etc. Though each of these terms has a specific meaning and scope, we use them relatively interchangeably. Here, we use these terms to refer to any company that maintains an online platform on which users interact, create content, or are otherwise connected to other users.

become tools for identifying, connecting with, and ultimately entrapping victims. It can happen on video games where people – often unsupervised children – use chat functions or audio or video streaming to engage with the people they play with.[3] Online "connections" can quickly become predatory real-life situations. These platforms can also be used by wrongdoers to facilitate sex trafficking. Social media platforms, websites that allow user-to-user advertisements, and even online games with live hosts can be used to solicit and advertise commercial sex.[4]

Entities that operate these platforms have long been protected from liability for this conduct by Section 230 of the Communications Decency Act. When Congress passed the Communications Decency Act of 1996, which sought to protect children by regulating obscenity and indecency online, it included a consequential provision – Section 230 – that has been interpreted as a broad liability shield for entities that provide "interactive computer service[s]."[5] Under current interpretations, Section 230 has effectively provided these entities with immunity from any suit based on the actions of other users on their platforms.[6] With Section 230, Congress intended to

[3] *See, e.g.*, Nellie Bowles & Michael H. Keller, *Video Games and Online Chats Are 'Hunting Grounds' for Sexual Predators*, N.Y. TIMES (Dec. 7, 2019, 12:33 PM), https://www.nytimes.com/interactive/2019/12/07/us/video-games-child-sex-abuse.html. Technological advances are also creating new and potentially even more troubling venues for predatory behavior. With virtual reality poised to enter mainstream social media, children who use these platforms may be at heightened risk of exploitation. *See* Will Oremus, *Kids are Flocking to Facebook's 'Metaverse.' Experts Worry Predators Will Follow*, WASH. POST (Feb. 7, 2022, 10:01 AM), https://www.washingtonpost.com/technology/2022/02/07/facebook-metaverse-horizon-worlds-kids-safety/.

[4] *See, e.g.*, M.L. v. Craigslist, No. C19-6153 BHS-TLF, 2020 U.S. Dist. LEXIS 166836, at *4-5 (W.D. Wash. Apr. 17, 2020) (describing plaintiff's claims that she was advertised to commercial sex purchasers on Craigslist by traffickers); Doe v. Backpage, 817 F.3d 12, 16 (1st Cir. 2016) (describing allegations that plaintiffs were trafficked as minors through advertisements posted on Backpage.com).

[5] 42 U.S.C. §230 (2018).

[6] *See* Jones v. Dirty World Entm't Recordings, LLC, 755 F.3d 398, 409 (6th Cir. 2014) (noting widespread adoption by courts of the principle that Section 230 bars claims that seek to hold an interactive service provider liable for information provided by a user where the defendant was not responsible for the creation of the information).

protect what it saw as an important but deeply vulnerable new industry: the internet.[7] Many believed that without this type of protection the internet would not be able to get off the ground because it would be so burdened by liability.[8]

The internet is no longer a fledgling industry though, and leaders from all fields – legislators, academia, judges, even the tech industry itself – seem to agree that Section 230 is untenable as it stands today. A recent article in the Harvard Business Review by Michael Smith and Marshall Van Alstyne, "It's Time to Update Section 230," summarized the common sentiment, arguing that the 1996 law is inadequate to address the challenges today's internet presents.[9] While Section 230 inherently accepted that some harms caused by the internet would be without redress, Smith and Van Alstyne suggest that "we significantly underestimated the cost and scope of harm" that can be caused online.[10] This type of commentary is not surprising given the nature of what some critics allege Section 230 has shielded, in particular, the online exploitation of highly vulnerable populations.[11]

Though Section 230 has long been the subject of controversy,[12] we are at an inflection point where imminent change is likely. Committees in the senate, including the Subcommittee on

---

[7] Christopher Cox, *The Origins and Original Intent of Section 230 of the Communications Decency Act*, RICH. J.L. & TECH. BLOG (Aug. 27, 2020), https://jolt.richmond.edu/2020/08/27/the-origins-and-original-intent-of-section-230-of-the-communications-decency-act/.

[8] *Id.*

[9] Michael D. Smith & Marshall Van Alstyne, *It's Time to Update Section 230*, HARV. BUS. REV. (Aug. 12, 2021), https://hbr.org/2021/08/its-time-to-update-section-230.

[10] *Id.*

[11] Doe, 817 F.3d at 16.

[12] *See* David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity under Section 230 of the Communications Decency Act*, 43 LOY. OF LOS ANGELES L. REV. 373, 373 (2010) ("In the thirteen years since its enactment, section 230 of the Communications Decency Act has become one of the most important statutes impacting online speech, as well as one of the most intensely criticized").

Consumer Protection, Product Safety, and Data Security and the Senate Committee on Homeland Security and Governmental Affairs, have held multiple hearings in recent sessions in which tech executives were interrogated about safety on their platforms.[13] The legislators have been transparent in their distaste for what they perceive as companies' failures to address the severe harms occurring online, and for the legal regime that they view as protecting them from accountability. In closing a hearing with executives from TikTok, Snapchat, and YouTube, Senator Markey said: "the problem is clear: Big Tech preys on children and teens to make money[.] Now is the time for the legislative solutions for these problems."[14] When closing a hearing in which Instagram executive Adam Mosseri testified, Senator Blumenthal said that the committee had a "pretty strong determination to do something" about this issue, and in response to some of Mosseri's proposed industry self-regulation, Blumenthal said the committee's actions would be "well beyond what you have in mind."[15] The National Association of Attorneys General wrote a letter to this subcommittee in October 2021 to express their "strong support" for these hearings.[16] The letter, signed by Attorneys General from all fifty states as well as Puerto Rico and Northern Mariana Islands, said: "When our

---

[13] *See, e.g.*, Alex Barinka, *Big Tech Critics in Senate Struggle to Turn Talk Into Action*, BLOOMBERG (Sept. 15, 2022, 6:45 AM), https://www.bloomberg.com/news/newsletters/2022-09-15/senate-hearings-for-tiktok-meta-twitter-youtube-lack-clear-path-forward ("Senators on both sides of the aisle finally agree on something: Social media needs to change."); *Social Media's Impact on Homeland Security: Hearing Before the S. Comm. on Homeland Sec. & Gov't Aff.,* 117th Cong. (2022); Vanessa Romo, *4 Takeaways from Senators' Grilling of Instagram's CEO about Kids and Safety*, NPR (Dec. 8, 2021, 10:13 PM), https://www.npr.org/2021/12/08/1062576576/instagrams-ceo-adam-mosseri-hears-senators-brush-aside-his-promises-to-self-poli; Kim Lyons, *Instagram Head Mosseri to Face Questions about Child Safety in Senate Hearing*, VERGE (Dec. 8, 2021, 9:51 AM), https://www.theverge.com/2021/12/8/22816730/mosseri-testimony-instagram-senate-hearing-haugen-child-safety-facebook-meta.

[14] Bobby Allyn, *4 Takeaways from the Senate Child Safety Hearing with YouTube, Snapchat and Tiktok*, NPR (Oct. 26, 2021, 6:38 PM), https://www.npr.org/2021/10/26/1049267501/snapchat-tiktok-youtube-congress-child-safety-hearing.

[15] Nicole Goodkind, *Senate Cracks Down on TikTok, Snapchat, and YouTube, Promising Legislative Action*, FORTUNE (Oct. 27, 2021, 12:15 PM), https://fortune.com/2021/10/27/senate-cracks-down-tiktok-snapchat-youtube-big-tech-legislation/.

[16] Letter from Nat'l Ass'n of Att'ys Gen. to U.S. Senate Comm. on Com., Sci., and Transp., Subcomm. On Consumer Prot., Prod. Safety, and Data Sec. (Oct. 4, 2021) (on file with ____).

young people's health becomes mere collateral damage of greater profits of social media companies, it is time for the government to intervene."[17] President Biden has also expressed his intention to tackle this issue by forming a task force to combat online harassment and abuse.[18] In his memorandum creating the task force, the White House specifically identified the use of online platforms for sex trafficking and sextortion as problems the task force should address.[19]

Section 230 has protected companies from significant liability for harms perpetrated online. But it appears that the floodgates will soon open – the only questions are how soon, and in what form. Bipartisan legislation has been proposed to limit Section 230's protections only to entities that take reasonable steps to prevent child exploitation.[20] Some have called for amending Section 230 more broadly by only granting immunity to entities that take "reasonable steps to address known unlawful uses of [their] services."[21] The Senate subcommittee on Consumer Protection, Product Safety, and Data Security is also preparing to introduce reform legislation. This legislative movement comes only a few years after the enactment of the Allow States and Victims to Fight Online Sex

[17] *Id.* at 2.

[18] Memorandum on the Establishment of the White House Task Force to Address Online Harassment and Abuse, THE WHITE HOUSE, June 16, 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/06/16/memorandum-on-the-establishment-of-the-white-house-task-force-to-address-online-harassment-and-abuse/.

[19] *Id.*

[20] *See* Committee on the Judiciary, *Graham, Blumenthal, Hawley, Feinstein Introduce EARN IT Act to Encourage Tech Industry to Take Online Sexual Exploitation Seriously*, Judiciary.Senate.Gov (Mar. 5, 2020) (https://www.judiciary.senate.gov/press/rep/releases/graham-blumenthal-hawley-feinstein-introduce-earn-it-act-to-encourage-tech-industry-to-take-online-child-sexual-exploitation-seriously).

[21] *See, e.g.*, Danielle Keats Citron and Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans §230 Immunity*, 86 FORDHAM L. REV. 401, 419 (2017).

Traffickers Act (FOSTA), which cut back Section 230 immunities in certain sex trafficking cases, and can be seen as a precursor to the much broader reform legislation that is likely to come.[22]

But change is also emerging from the judicial branch. The breadth of 230's immunity comes in large part from expansive interpretations of the statute, not from language in the statute itself.[23] In some recent cases, judges have chipped away at this expansiveness and found ways to permit claims against platform hosts to go forward.[24] And while state and lower federal courts are constrained by prevailing interpretations of the law, the Supreme Court has yet to interpret Section 230. It will do so for the first time in the upcoming session.[25] Justice Thomas has already signaled his views by stating that the Supreme Court should reconsider the expansiveness that has been read into Section 230.[26] A Supreme Court decision reinterpreting Section 230 could immediately open platform hosts up to substantial liability.

While unknowns remain, some things are certain. Human trafficking and child exploitation online are massive problems, and they are getting worse. Anyone operating a platform where users interact can inadvertently facilitate these crimes through inaction or through methods that are employed to enhance user experience and generate revenue but also advance criminal activity. Until

---

[22] Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, §2, 132 STAT. 1253, 1253 (2018).

[23] *See, e.g.*, Doe v. Facebook, 595 U.S. ___, at *3 (2022) (statement of Thomas, J., respecting denial of certiorari) ("[a]ssuming Congress does not step in to clarify Section 230's scope, we should do so in an appropriate case."); *see also* Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 15 (2020) (statement of Thomas, J., respecting denial of certiorari) (internal citations omitted) ("Adopting the too-common practice of reading extra immunity into statutes where it does not belong,. . .courts have relied on policy and purpose arguments to grants sweeping protection to Internet platforms.").

[24] *See, e.g.*, In re Facebook, 623 S.W.3d 80, 101 (Tex. 2021) (holding that state law sex trafficking claims against Facebook were not barred by Section 230).

[25] Gonzalez v. Google, 214 L. Ed 2d 12 (S. Ct. 2022)

[26] Malwarebytes, Inc. v. Enigma Software Grp. U.S., 141 S. Ct. 13, 14 (2020).

now, that risk has been carried by users themselves – those who become victims have few options for recourse. But policymakers at all levels are determined to reallocate that risk, and entities operating online will soon have a legal obligation to take measures to prevent these crimes. Failing to do so will be costly – both in the financial costs of liability and in the reputational harms that follow the public failure to protect vulnerable users from becoming victims.

2. **The Growing Problems of Human Trafficking and Child Exploitation Online**

(a) The Magnitude and Scope of the Problem

Social media and other online platforms have become a habitat for individuals who seek to entice and exploit children and recruit victims for trafficking in sex. Although it's difficult to precisely ascertain the prevalence of online sexual exploitation crimes, including sex trafficking offenses, one mechanism by which prevalence is measured is by examining the National Center for Missing and Exploited Children's (NCMEC's) CyberTipline, created in 1998 to serve as an online means for individuals and electronic service providers (ESPs) to report suspected child sexual exploitation.[27] Since 1988, the CyberTipline has received over 92 million reports.[28] The volume of reports has grown with the use of the internet. In 1999, the CyberTipline received less than 10,000 reports; in 2014, it received over 1 million reports; in 2019, it received nearly 17 million reports; and in 2020, it received over 21 million reports.[29] The emergence and popularity of chat and messaging services has led to more complex reports that include enticement and grooming, along with the distribution of child

[27] National Center for Missing and Exploited Children, *The Attorney Manual to Guide Representation of Children Victimized by Online Distribution of Sexual Abuse Material,* 7 (2021) (https://www.missingkids.org/content/dam/missingkids/pdfs/NCMEC%20Restitution%20Manual%20Final.pdf).

[28] *Id.*

[29] *Id.*; *see also* Detailed 2019 and 2020 Statistics, NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN, 2022, https://www.missingkids.org/gethelpnow/cybertipline#bythenumbers.

pornography and/or sextortion.[30] Overall, the dominant type of report to the CyberTipline relates to child pornography, but notably from 2019 to 2020, reports to NCMEC related to the enticement of children for sex were up an astonishing ninety-seven (97) percent.[31]

The use of the internet to recruit trafficking victims has similarly increased.[32] Between 2015 and 2018, the U.S. National Human Trafficking Hotline documented "almost 1,000 cases of potential victims of sex trafficking alone who were recruited through internet platforms, most often Facebook, but also Instagram, Snapchat, Craigslist, online dating sites, and chat rooms."[33] The Hotline recorded close to 11,000 trafficking "instances" in 2018 and 11,500 "instances" of trafficking in 2019.[34] Although these statistics include both sex and labor trafficking, the dominant trafficking type domestically is sex trafficking.[35] The NCMEC CyberTipline recorded almost 16,000 complaints related to child sex trafficking.[36]

---

[30] National Center for Missing and Exploited Children, *supra* note 27.

[31] National Center for Missing and Exploited Children, Cyber Tipline, https://www.missingkids.org/gethelpnow/cybertipline [hereinafter NCMEC Cyber Tipline]. NCMEC defines online enticement as: "an individual communicating with someone believed to be a child via the internet with the intent to commit a sexual offense or abduction and includes crimes like sextortion."

[32] *See* UN News, *Traffickers Abusing Online Technology, UN Crime Prevention Agency Warns*, UNITED NATIONS (Oct. 30, 2021), https://news.un.org/en/story/2021/10/1104392.

[33] Melissa Withers, *Social Media Platforms Help Promote Human Trafficking*, Psychology Today (Nov. 22, 2019), https://www.psychologytoday.com/us/blog/modern-day-slavery/201911/social-media-platforms-help-promote-human-trafficking.

[34] Polaris, *2019 Data Report; The U.S. National Human Trafficking Hotline*, https://humantraffickinghotline.org/sites/default/files/Polaris-2019-US-National-Human-Trafficking-Hotline-Data-Report.pdf.

[35] *Id.*

[36] NCEM CyberTipline, *supra* note 31.

The proliferation of the use of online platforms to recruit both children and adults to engage in commercial sex has been documented in the United States and in countries around the world.[37] The 2021 State Department Trafficking in Persons (TIP) Report summarized its findings:

> [The pandemic] forced many people to shift online, including human traffickers. . . . Reports from several countries demonstrated drastic increases in online commercial sexual exploitation and sex trafficking, including online sexual exploitation of children (OSEC), and demand for and distribution of child sexual exploitation material (CSEM), including content that involved human trafficking victims. The Philippine Department of Justice noted an increase of nearly 300 percent in referrals for potential online sex trafficking and OSEC cases from March to May 2020, the period during which the Philippines was under lockdown or quarantine measures. In India, there was a reported 95 percent rise in online searches for CSEM, and India ranked among the highest countries in the world for material related to child sexual abuse found online with a total of 11.6 percent of a global compilation of reports in 2020. . . . While traffickers used the opportunity of increased numbers of children online to expand their operations, it should be noted that a portion of the increase resulted from the recirculation of sensationalized trafficking-related stories and misinformation on social media platforms. This included individuals who reshared CSEM content in hopes of helping the victim and raising awareness, but inadvertently contributed to reporting spikes leaving less time and resources to pursue every incident.[38]

The TIP report identifies numerous countries where criminals are using social media and other online tools to recruit victims for sex trafficking including Argentina, Austria, Belarus, Denmark, Germany, Hong Kong, Indonesia, Namibia, Norway, Spain, and Taiwan.[39] In the Philippines, criminals are sexually exploiting children live on the internet for money.[40] Although the pandemic may have decreased some forms of sexual abuse, it was simply replaced by online exploitation. For example, in Cambodia, although child sex tourism predictably declined during the pandemic, the

[37] Withers, *supra* note 33.

[38] Department of State, *Trafficking in Persons Report*, 7 (June 2021), https://www.state.gov/reports/2021-trafficking-in-persons-report/.

[39] *Id*. at 91, 98, 118, 211, 253, 276, 293, 408, 433-34, 516, and 537.

[40] *Id*. at 454, 458.

country experienced an increase in online child sexual exploitation.[41] In France, sex traffickers increasingly used online platforms to recruit and exploit victims; non-governmental organizations estimated that more than half of the commercial sex encounters were organized online.[42]

Online platforms are also used to perpetuate labor trafficking around the world. In countries including Guatemala, India, Kenya, Kyrgyz Republic, Liberia, Thailand, and Turkey, criminals took to the internet to recruit victims for both sex and labor trafficking.[43] The TIP report describes an example of this conduct in Brazil:

> Migrants and people living near any of Brazil's border areas are vulnerable to trafficking. Traffickers have exploited Chinese women in sex trafficking in Rio de Janeiro. Venezuelan migrants within Brazil were highly vulnerable to sex trafficking and forced labor. Traffickers recruit Venezuelans—those living in Brazil and those still in Venezuela—via online advertisements and social media platforms offering fraudulent job opportunities, later exploiting them in sex trafficking in major cities like Sao Paulo and Rio de Janeiro.[44]

Recent events highlight some of the legal and reputational dangers to companies for allegedly failing to identify, block, and remove from its platforms content relating to labor trafficking, in particular domestic servitude content posted by users outside the United States.[45]

Child predators and sex traffickers have expanded their reach beyond well-known social media platforms to virtual spaces once thought to be relatively safe for vulnerable populations. Criminals are reaching into the homes of unsuspecting parents, engaging children online through

---

[41] *Id*. at 161.

[42] *Id*. at 242.

[43] Department of State, *supra* note 38 at 261, 287, 331, 346, 357, 548-49, and 565.

[44] *Id*. at 139.

[45] *See* Clare Duffy, *Facebook has Known it Has a Human Trafficking Problem for Years. It Still Hasn't Fully Fixed It*, CNN (Oct. 25, 2021, 7:33 AM), https://www.cnn.com/2021/10/25/tech/facebook-instagram-app-store-ban-human-trafficking/index.html.

multiplayer video games and chat applications.[46] Wrongdoers "strike up a conversation and gradually build trust. Often, they pose as children, confiding in their victims with false stories of hardship or self-loathing. Their goal, typically, is to dupe children into sharing sexually explicit photos and videos of themselves — which they use as blackmail for more imagery, much of it increasingly graphic and violent."[47] Criminals have and will continue to infiltrate well-intended social media services, messaging applications, and other online engagement platforms such as those designed to help individuals find a roommate, a date, or a study group.[48] Online gambling applications are likely to encounter similar difficulties. Unfortunately, history has shown that any online communication tool, particularly one that includes personal messaging, is susceptible to the risk that bad actors will utilize it to identify, groom, and entice children for illegal activity or recruit children and adults to be trafficked for sex or labor. Similarly, any online service that permits and benefits from advertising on its site opens itself to the potentiality that users will recruit victims and/or advertise illegal services on its platform.

(b) Applicable U.S. Law

[46] Bowles and Keller, *supra* note 3. *See also* Federal Bureau of Investigation (FBI), *Child Predators Use Online Gaming to Contact Children*, Public Service Announcement (Dec. 12, 2019) (https://www.ic3.gov/Media/Y2019/PSA191212).

[47] Bowles and Keller, *supra* note 3.

[48] This phenomenon has been documented inside and outside the United States. For example, the State Department TIP report notes that, "Israeli children, Israeli Bedouin and Palestinian women and girls, foreign women, and transgender adults and children are vulnerable to sex trafficking in Israel. Traffickers use social media websites, including dating apps, online forums and chat rooms, and Facebook groups, to exploit girls in sex trafficking." Department of State, *supra* note 38, at 310. In Lithuania, "traffickers have shifted recruitment methods from in-person to online settings, mainly through social media, hindering authorities' ability to locate victims and identify traffickers." *Id.* at 360. In Mongolia, traffickers use job postings and English language programs to lure unsuspecting victims into sex trafficking. *Id.* at 400. In the United States, offenders take the same approach. *See* U.S. Department of Justice, Press Release, Shelby County Man Sentenced to 27 Years in Prison for Sending Money to Filipino Mothers in Exchange for Child Pornography (Nov. 5, 2021), available athttps://www.justice.gov/usao-sdoh/pr/shelby-county-man-sentenced-27-years-prison-sending-money-filipino-mothers-exchange (defendant met impoverished mothers on dating sites and paid them for access to sexual images of their children).

There are numerous laws at the Federal and state level that criminalize various forms of sexual abuse, exploitation, and human trafficking. This section focuses on Federal law – and in particular those laws that especially implicate conduct that occurs online - but it is likely (although not always the case) that if certain conduct violates Federal law, it similarly violates the law of the State in which the criminal act(s) occurred. Notably, different jurisdictions may criminalize slightly different conduct and the age of adulthood or consent can differ by jurisdiction. Under Federal law, an individual is considered a minor until the age of 18.[49] Recent civil actions brought by victims based on exploitative online content generally allege violations of Federal law, the relevant law of the state at issue, and negligence claims. As discussed in greater detail below, some of those actions have been successful and victims will likely continue to succeed beyond the motion to dismiss stage in certain of these actions.[50]

Sections 2251, 2252, and 2252A, criminalize the production, distribution, advertising, receipt and possession of child pornography. Child pornography is a visual depiction (for example, a picture or a video) that shows a minor engaged in sexually explicit conduct.[51] "Sexually explicit conduct" includes most sex acts and the "lascivious exhibition" of certain body parts.[52] Section 2260 criminalizes the production of child pornography, including live visual content, outside the United States, if the person intended that the content would be imported or transmitted into the United States.[53] Section 2422(b) criminalizes the persuasion or enticement of a minor using any means of

[49] 18 USC § 2256.

[50] *See* Doe v. Twitter, Ic., No. 21-CV-00485-JCS, 2021 U.S. Dist. LEXIS 157158, (N.D. Cal. Aug. 19, 2021)(holding that plaintiffs could survive motion to dismiss based on trafficking beneficiary liability under Section 1591(a)(2)); *see also* In re Facebook, 625 S.W.3d 80 (Tex.. 2021)(denying writ of mandamus seeking dismissal of trafficking claim against social media company).

[51] 18 U.S.C. §§2251, 2252, 2252A, 2256(8).

[52] 18 U.S.C. §2256(2).

[53] 18 U.S.C. §2260.

interstate commerce (e.g., the internet) to engage in prostitution or any sex act for which a person can be charged with a crime.[54] Section 2255 authorizes a private cause of action for victims of Federal exploitation crimes if those crimes occurred while they were minors, including crimes relating to sexual abuse, child pornography, sex and labor trafficking, and enticement.[55] The statute authorizes the award of actual damages, attorney's fees and costs, punitive damages, and "such other preliminary and equitable relief as the court determines appropriate."[56]

The Trafficking Victims Protection Act (TVPA) defines human trafficking, or "severe forms of trafficking in persons," as sex trafficking in which a commercial sex act is induced by force, fraud, or coercion, or in which the person induced to perform such act is under the age of 18; and the recruitment, harboring, transportation, or obtaining of a person for labor or services, through the use of force, fraud, or coercion.[57] The primary Federal criminal prohibition on sex trafficking is found in 18 U.S.C 1591, which criminalizes recruiting, enticing, or obtaining a person for commercial sex if the person is a minor, or if force, fraud, or coercion is used, or if a person benefits financially from participation in a venture involving commercial sex acts prohibited by the statute.[58] Some trafficking cases involve the physical movement of victims across state lines. In those cases, prosecutors may also charge Section 2421, which prohibits the transportation of a person across state lines for prostitution or sexual activity for which any person can be charged with a crime.[59] Labor trafficking is criminalized by 18 U.S.C. 1589. The statute prohibits knowingly providing or

[54] 18 U.S.C. §2422(b).

[55] 18 U.S.C. §2255.

[56] *Id.*

[57] Office of the Attorney General, Attorney General's Report to Congress on Trafficking in Persons vii (2018) https://www.justice.gov/d9/pages/attachments/2020/05/13/agtipreport-fy2018.pdf.

[58] 18 U.S.C. §1591.

[59] 18 U.S.C. § 2421.

obtaining the services of another through force, fraud, or coercion.[60] The statute also creates criminal liability for those who benefit financially or receive anything of value from knowingly participating in a venture that has engaged in labor trafficking.[61] Section 1595 creates a civil cause of action against traffickers or those who knowingly benefit or profit from trafficking.[62] A victim is entitled to damages and reasonable attorney's fees.[63]

3. **The Shifting State of Liability for Web-Based Platforms**

Any entity that operates an online platform that can be used by wrongdoers involved in child exploitation or human trafficking is at risk of liability – even if the host did not have a specific intent to facilitate the conduct. Until recently, protective interpretations of Section 230 of the Communications Decency Act have provided a nearly impenetrable shield to internet service providers for the actions of their users. [64] But change is likely coming. Legislative amendments and recent legal opinions applying Section 230 less protectively have opened new doors to liability. Future legislative activity is likely to place more responsibility on entities to protect users from the harms that can be perpetuated on their web platforms – and to impose liability on those who fail to do so.

Legislators from across the political spectrum have proposed amending Section 230 – or replacing it altogether.[65] One such amendment, the Allow States and Victims to Fight Online Sex

---

[60] 18 U.S.C. § 1589.

[61] *Id.*

[62] 18 U.S.C. §1595 (2018).

[63] *Id.*

[64] *See* Zeran v. America Online, Inc., 129 F.3d 327, 334 (4th Cir. 1997), cert. denied, 524 U.S. 937 (1998) ("Congress' desire to promote unfettered speech on the Internet must supersede conflicting common law causes of action.").

[65] *See, e.g.*, Zoe Bedell & John Major, *What's Next for Section 230? A Roundup of Proposals*, LAWFARE (Jul. 29, 2020), https://www.lawfareblog.com/whats-next-section-230-roundup-proposals.

Trafficking Act (FOSTA), was already passed to eliminate 230's liability shield in some cases where platforms facilitate sex trafficking.[66] Broad interpretations of Section 230 have also been called into question by recent case law.[67] The Supreme Court will interpret Section 230 for the first time in its upcoming session,[68] and as consensus on the breadth of the protection the law provides erodes over time, it is positioned to craft a much narrower interpretation than has existed to date.[69] With a formal proposal for changes to Section 230 from the Department of Justice (DOJ),[70] all three branches of government have weighed in. And all have signaled a move away from providing web-based platforms with the level of broad protection from liability that they have today. Thoughtful entities that seek to launch new services and companies currently operating in this space should be aware of these potential legal and statutory changes and prepare to take a more active role in policing their platforms to avoid potential liability and reputational damage.

(a) Overview and History of Section 230

For the past twenty-five years, the question of whether web-based platforms are liable for harms perpetrated on their sites has been governed by Section 230 of the Communications Decency Act.[71] Passed as the internet was just rising to prominence, Section 230 represented Congress's efforts to allow the internet to grow by protecting companies operating web-based platforms from

[66] Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, §2 (2018).

[67] *See* In re Facebook, 625 S.W.3d 80, 91-93 (Tex. 2021) (denying motion to dismiss under Section 230 immunity as it relates to state law sex trafficking claims).

[68] Gonzalez v. Google, 214 L. Ed 2d 12 (S. Ct. 2022).

[69] *See, e.g.*, Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 15 (2020) (statement of Thomas, J., respecting denial of certiorari) (acknowledging that the prevailing interpretation of Section 230 is not the only plausible understanding).

[70] Dep't of Just., Office of Public Affairs, The Justice Department Unveils Proposed Section 230 Legislation, DEP'T OF JUST. (Sept. 23, 2020), https://www.justice.gov/opa/pr/justice-department-unveils-proposed-section-230-legislation.

[71] 47 U.S.C. §230(c)(1) (2018).

exposure to excessive liability.[72] Congress also sought, through Section 230, to encourage internet service providers to moderate content on their platforms by shielding them from liability in the event that their moderation efforts failed to prevent harm.[73] From the time of its enactment, Section 230 was interpreted broadly and has been the basis of countless 12(b)(6) dismissals.[74]

Congress passed Section 230 in direct response to a pair of defamation cases whose outcomes created a disincentive for websites to moderate harmful content.[75] In both cases, a defendant-company was sued for defamatory content that a third-party posted on a forum hosted by the defendant.[76] In the first case, the defendant engaged in no content moderation; posts by users were automatically uploaded to the forum.[77] In the second case, the defendant sought to operate a family-friendly forum by screening posts and attempting to remove any offensive content posted by users.[78] Under principles of defamation law, this difference in moderation practices meant that the first defendant was considered a distributor while the second defendant was a publisher.[79] Distributors – like bookstores and libraries – are not liable for defamatory content they distribute unless they had actual knowledge of the defamatory material.[80] By contrast, publishers – like newspapers and magazines – are liable for the content they publish because they are expected to

---

[72] *See* Cox, *supra* note 7.

[73] *Id.*

[74] *See, e.g.*, Malwarebytes, 141 S. Ct. at 15-18 (describing the "broad array" of cases in which Section 230 has protected defendants from liability); *See* discussion *infra*, Section 3a.

[75] Cox, *supra* note 7, at 25.

[76] Cubby, Inc. v. Compuserve, 776 F. Supp. 135, 137 (S.D.N.Y. 1991); Stratton Oakmont v. Prodigy Servs. Co., No. 31063/94, 1995 N.Y. Misc. LEXIS 229, at *2 (N.Y. Sup. Ct. May 26, 1995).

[77] *Cubby*, 776 F. Supp. at 137.

[78] *Stratton Oakmont*, 1995 N.Y. Misc. LEXIS 229, at *3-4.

[79] *Id*. at *10-11.

[80] Cubby, 776 F. Supp. at 139.

have knowledge of the content over which they exercise editorial discretion.[81] This meant that companies could avoid liability as long as they made no effort to keep harmful content off of their platforms.

Section 230 responded to these cases with two provisions. The first, Section 230(c)(1), states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[82] The second, Section 230(c)(2), states:

> "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, harassing, 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 paragraph (1)."[83]

Though there are a few ways these provisions could be interpreted, courts were unanimous in reading them to be broadly protective of internet companies.[84] In the first case interpreting Section 230, *Zeran v. Am. Online*, the Fourth Circuit held that 230(c)(1) did not just eliminate publisher liability in defamation cases, but it prohibited distributor liability as well.[85] Since *Zeran*, every circuit

[81] Stratton Oakmont, 1995 N.Y. Misc. LEXIS 229 at *7.

[82] 47 U.S.C. § 230(c)(1) (2018).

[83] 47 U.S.C. § 230(c)(2) (2018).

[84] *See* Zeran v. Am. Online, 129 F.3d 327, 331 (4th Cir. 1997)(describing §230 as providing "broad immunity"); Malwarebytes, 141 S. Ct. at 15 (stating that "subsequent decisions, citing *Zeran*, have adopted this holding as a categorical rule across all contexts.").

[85] Zeran, 129 F.3d at 333.

has held that Section 230 shields internet platforms from any liability – not just under defamation theories –based on content generated by third parties.[86]

Under *Zeran* and cases that followed, companies operating web-based platforms could rely on 230 as a complete liability shield as long as (1) they are an interactive service provider, (2) the plaintiff seeks to hold them liable as a publisher or speaker, and (3) the plaintiff's claim arises from content provided by another information content provider.[87]

These broad interpretations of Section 230 have effectively meant that companies were not liable for human trafficking or child exploitation perpetrated on their platforms. Courts have routinely dismissed cases where defendants allegedly facilitated human trafficking by knowingly allowing traffickers to use their sites for advertisements, and even cases where defendants designed sections of their platforms to meet the needs of traffickers.[88] When wrongdoers have used social media sites and dating apps to identify, contact, and entrap victims, those platforms have avoided liability because they did not create the content that caused the harm.[89]

Section 230 has also protected companies that refused to act to address severe harms being perpetrated on their platforms.[90] For example, in *Doe v. Mark Bates & Yaloo!, Inc.*, plaintiffs accused Yahoo of knowingly hosting a forum where users shared child pornography.[91] Yahoo "did nothing to prevent, remove, or block" the child pornographic material it allegedly knew was on its

[86] Malwarebytes, 141 S. Ct. at 15.

[87] Jones v. Dirty World Entm't Recordings LLC, 755 F.3d 398, 409 (6th Cir. 2014).

[88] *See* Doe v. Backpage, 817 F.3d 12, 21 (1st Cir. 2016) (granting §230 immunity in spite of allegations that the company "deliberately attempt[ed] to make sex trafficking easier" because the defendant's motivations do not affect the applicability of §230).

[89] *See, e.g.*, Herrick v. Grindr, 765 Fed. Appx. 586, 590-91 (2d Cir. 2019)(dismissing claim against dating-app defendant for harassment because the harms resulted from another user's impersonating content).

[90] *See, e.g.*, Doe v. Twitter, 555 F. Supp. 3d 889, 930-32 (N.D. Cal. 2021).

[91] Doe v. Bates, No. 5:05CV91, 2 (Dkt. No. 56) (E.D. Tex Jan. 18, 2006), report and recommendation adopted, 2006 U.S. Dist. LEXIS 93348 (E.D. Tex. Dec. 27, 2006).

platform.[92] Claims arising from this failure to address illegal material were barred by Section 230 because they sought "to hold [Yahoo] liable for its exercise of a publisher's traditional editorial functions."[93] The court expressly rejected an argument that intentional violations of criminal law were exempt from 230 immunity.[94] Similarly, in *Herrick v. Grindr*, the Second Circuit held that Section 230 barred claims based on stalking and harassment the plaintiff suffered when a dating application refused to remove accounts impersonating him.[95]

Section 230 immunity has also consistently shielded companies against product liability suits claiming that companies had an obligation to implement safety features or provide warnings to users in the face of known risks. In *Doe v. Myspace*, Myspace's failure to implement measures to prevent predators from connecting with minors on the platform was protected by Section 230 because liability would be based on Myspace's publishing of the predators' content and messages.[96] The Southern District of Florida applied similar reasoning in *Doe v. Kik Interactive*, holding that Section 230 barred claims that the messaging app was at fault for predatory behavior because it lacked sufficient safety features.[97]

Although it was not a matter of dispute that the defendants could have done more to address trafficking and child exploitation on their platforms, the broad interpretation of Section 230

[92] *Id.* at 4.

[93] Doe v. Mark Bates & Yahoo!, Inc., No. 5:05-CV-91-DF-CMC, 2006 U.S. Dist. LEXIS 93348, at *9 (E.D. Tex. Dec. 27, 2006).

[94] *Id.*

[95] Herrick v. Grindr LLC, 765 F. App'x 586, 591 (2d Cir. 2019).

[96] Doe v. Myspace, 528 F.3d 413, 419-20 (5th Cir. 2008). *See also Twitter*, 555 Fed. Supp 3d, 929-31 (dismissing products liability claim against Twitter under the same reasoning).

[97] Doe v. Kik Interactive, 482 F. Supp. 3d 1242, 1251 (S.D. Fla. 2020).

followed by the courts meant they had no obligation to take those steps and bore no liability to victims of the offenses perpetrated on the platform.[98]

(b) Cracks in the Shield: The Liberalization of 230

But recent court opinions, academic thinking, and enacted and proposed legislation evidence a shift in thinking. Courts are now suggesting that companies with the resources to reduce the risks they create are responsible for doing so, at least with respect to human trafficking and child exploitation. There is near-universal consensus on the abhorrent nature of sex trafficking, particularly of minors, which makes it difficult to adopt a doctrine that protects those who facilitate it. The First Circuit acknowledged this in the first line of *Doe v. Backpage.com*, a case where the facts indicated that the defendants had intentionally facilitated the sex trafficking of minors: "This is a hard case … in the sense that the law requires that we … deny relief to plaintiffs whose circumstances evoke outrage."[99] For many years the policy behind Section 230 – Congress's wish to protect the fledgling internet from being destroyed by excessive liability – provided some balance against the ethical weight of erring on the side of internet service providers against victims of abuse. But now these companies are often powerful and resource-rich organizations whose imminent collapse seem unlikely. Recent legislation and case law show that policymakers and judges have begun to question and even crack the broad liability shield, requiring these companies act to prevent their platforms from facilitating human trafficking or disseminating child exploitation materials.

(i) Enacted Legislative Change: Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA)

Congress amended Section 230 in 2018 with the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA), which created an exception to the 230 liability shield for conduct that

[98] *See, e.g.*, Myspace, 528 F.3d at 421 (describing available technology that would have prevented minors from misrepresenting their ages on social media).

[99] Doe v. Backpage, 817 F.3d 12, 15 (1st Cir. 2016).

violates the Federal sex trafficking statute.[100] Although FOSTA has not been tested extensively,[101] it provides grounds for plaintiffs to successfully navigate around the Section 230 liability shield if the underlying conduct is pled as sex trafficking. Under one line of interpretation, FOSTA may revive an equivalent to the distributor liability rejected by the *Zeran* court by triggering liability when companies fail to adequately respond to reports of sex-trafficking-related content. FOSTA may also create obligations under a constructive notice theory, requiring companies whose services are likely used by traffickers to take steps to reduce this risk.

As it relates to civil liability, FOSTA amends Section 230 to state: "Nothing in this section (other than subsection (c)(2)(A)) shall be construed to impair or limit … 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[.]"[102] Section 1595 creates a civil cause of action for victims of a certain subset of crimes, including Section 1591,[103] which criminalizes sex trafficking of children and sex trafficking by force, fraud, or coercion.[104]

The most significant opportunity FOSTA creates for plaintiffs is beneficiary liability. Under FOSTA, victims can avoid the Section 230 bar if they plead that a company benefitted from participating in a venture with sex traffickers. A benefit can be shown by a claim that companies

---

[100] Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, §2, 132 Stat. 1253, 1253 (2018).

[101] According to a June 2021 report by the Government Accountability Office, only one plaintiff had sought civil damages under FOSTA since the law was enacted, and that plaintiff was not successful. U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-385, SEX TRAFFICKING: ONLINE PLATFORMS AND FEDERAL PROSECUTIONS 25 (2021). There have been a select few cases invoking FOSTA since this report. *See, e.g.*, *In re Facebook*, 623 S.W.3d 80 (Tex. 2021)(invoking FOSTA in attempt to avoid dismissal based on CDA immunity); *Twitter*, 555 Fed. Supp. 3d at 898. (same).

[102] §4, 132 Stat. at 1254.

[103] 18 U.S.C. §1595.

[104] 18 U.S.C. §1591.

usually profit from the engagement with their platform that the illicit content drives.[105] But case law is sparse thus far on the trickier question of what type of relationships platforms must have with traffickers to invoke this type of liability. It also remains unclear whether companies must affirmatively know of the trafficking to be liable, or whether companies may be liable under the theory that they should have known about the conduct. Though theoretically distinct, on occasion these two questions have been assessed together such that when a platform is alleged to have actual knowledge of trafficking content, its failure to react appropriately leads the court to find a sufficient relationship between the platform and the traffickers. This result could revive an equivalent of distributor liability for these entities.

Two cases, *Doe v. Twitter* and *Doe v. Reddit*, demonstrate FOSTA's potential to open service providers to liability based on how they respond to reports of illegal content on their platform.[106] In both cases, the plaintiffs sued for damages as a result of sexually explicit images and videos of underage victims being posted on the defendants' platforms.[107] In *Reddit*, images and videos of the

[105] *See, e.g.*, Twitter, 555 Fed. Supp. 3d at 924-25 (finding that Twitter benefitted from the tweeting and retweeting of child pornography based on Twitter's practices of monetizing content "through advertising, sale of access to its API, and data collection.").

[106] The significance of these cases may be affected by the Ninth Circuit's recent ruling in *Does v. Reddit*, where it affirmed the dismissal of claims against Reddit. *Does v. Reddit*, No. 21-56293, 2022 U.S. App. LEXIS 29510, _ F. 4th _ , at *20 (9th Cir. 2022). The Ninth Circuit held that FOSTA applies only when a defendant is alleged to have actively participated in sex trafficking - but not if they merely "turn[] a blind eye" to it. *Id*. The court found that the allegations against Reddit amounted only to turning a blind eye and perhaps consequently provided little insight into what constitutes "active participation." *Id*. The district court opinions in *Twitter* and *Reddit* may therefore continue to be useful to understand how a platform's alleged awareness of trafficking content will affect a court's assessment of its participation in the trafficking venture.

[107] Doe v. Reddit, No. SACV 21-769 JVS(KESx), 2021 U.S. Dist. LEXIS 129876, at *12-13 (C.D. Cal. Jul. 12, 2021); Twitter, 555 Fed. Supp. 3d at 894. It is worth noting that in both of these cases, plaintiffs stretched to plead their allegations as sex trafficking claims under §1591. This was necessary because FOSTA only exempts claims from §230 immunity if the underlying conduct violates §1591. Ultimately, defendants may be able to successfully argue that FOSTA does not apply because the underlying conduct does not violate §1591, which includes a commercial sex element. Nonetheless, courts have not evaluated this argument at the motion to dismiss stage, and especially in cases involving child sexual abuse, the process of establishing which federal statute was violated may be a painful one.

plaintiffs were repeatedly posted on the site's forums.[108] Reddit removed the posts when the plaintiffs reported them.[109] The plaintiffs complained, however, that Reddit did not do enough to prevent the repeated re-posting of the images and videos.[110] By contrast, when the *Twitter* plaintiffs reported the posts at issue, Twitter denied the request that the posts be removed.[111]

Under the pre-FOSTA *Zeran* interpretation of Section 230, both of these cases would have been dismissed. The *Zeran* court explicitly rejected the argument that the defendant's refusal to remove harmful content of which it was aware could be the basis of liability.[112] According to the *Zeran* court, this type of "notice-based liability" would create too significant of a burden on interactive service providers to respond to complaints because of the sheer volume of content that could be reported as harmful.[113] For this reason the *Zeran* court – and all courts that subsequently faced this question – held that Section 230 prevented web-based platforms from being held liable as distributors when they knowingly host illegal content.[114]

Twitter and *Reddit* may indicate a revival of the notice-based liability rejected by the *Zeran* court. The *Twitter* claims survived a motion to dismiss based on 230 immunity, while the *Reddit* claims were dismissed.[115] Because both claims were based on FOSTA beneficiary liability, the key difference was whether the defendants were alleged to have participated in a venture with the

[108] Reddit, 2021 U.S. Dist. LEXIS 129876, at *3.

[109] *Id*.

[110] *Id*.

[111] Twitter, 555 F. Supp 3d at 893.

[112] Zeran, 129 F.3d at 333.

[113] *Id*.

[114] *Id*.; *See also* Twitter, 555 F. Supp 3d at 927 (agreeing with *Zeran*'s holding that Section 230 bars claims that platforms should have removed content once they are informed of its illegal nature).

[115] *Twitter*, 555 F. Supp 3d at 925; Doe v. Reddit, No. SACV 21-769 JVS(KESx), 2021 U.S. Dist. LEXIS 129876, at *19 (C.D. Cal. Jul. 12, 2021).

traffickers. Establishing that a defendant participated in a venture requires "a showing of a continuous business relationship between the trafficker and the defendant such that it would appear that the trafficker and the defendant have established a pattern of conduct or could be said to have a tacit agreement."[116] In *Reddit*, the only relationship alleged was that Reddit furthered trafficking by enabling traffickers to post child pornography, which made it easier to connect traffickers with those who want to view child pornography.[117] The court wrote that if this were sufficient to establish participation in a venture, it "would mean that all web-based communications platforms have a legal duty to inspect every single user-generated message before it is communicated [.]"[118] In *Twitter*, however, the court relied on the fact that Twitter chose not to remove content after it had been informed that it contained child pornography.[119] It was also relevant that another user had reported the posting account as one that posts child pornography.[120] Because Twitter had been informed that the account and the posts involved child pornography and it did not remove the post or disable the account, the Court found that the plaintiff sufficiently pled that Twitter had participated in a venture with the traffickers.[121] The FOSTA beneficiary claim therefore survived a motion to dismiss.[122]

Though *Twitter* and *Reddit* came to opposite results, their implications for beneficiary liability doctrine are coherent; they suggest that a failure to remove trafficking content can be sufficient to participate in a venture with traffickers. Future plaintiffs in cases with similar facts to *Reddit* will

---

[116] *Reddit,* 2021 U.S. Dist. LEXIS 129876, at *12 (*quoting J.B. v. G6 Hosp., LLC*, No. 19-cv-07848-HSG, 2020 U.S. Dist. LEXIS 151213, at *9 (N.D. Cal. Aug. 20, 2020)).

[117] *Id.* at *12-13.

[118] *Id.* at *13.

[119] Twitter, 555 F. Supp 3d at 922.

[120] *Id.* at 922-23.

[121] *Id*. at 923.

[122] *Id*. at 925.

likely be able to survive a motion to dismiss if they draft their complaint to mirror the allegations made in *Twitter*.

Courts may treat defendants as having knowledge of sex trafficking in cases where they should have been aware of it; establishing actual knowledge may not be necessary for participation in a venture. This is particularly relevant where wrongdoers use platforms' tools to further their illicit purposes. Before FOSTA was enacted, Section 230 protected companies from liability when criminals used their neutral tools to facilitate crimes.[123] For example, in *Herrick v. Grindr*, Section 230 shielded the defendant dating application from liability for a stalker's use of the app's geolocation feature to impersonate and harm the plaintiff.[124] The court wrote that Grindr "cannot be held liable for providing 'neutral assistance' in the form of tools and functionality available equally to bad actors and the app's intended users."[125]

There is reason to believe, however, that this neutral assistance reasoning will not be applied as protectively in FOSTA cases where defendants had reason to know that their tools could be used in furtherance of sex trafficking. This issue arose in *In re Facebook*, where the plaintiffs alleged that Facebook assisted sex traffickers by, *inter alia*, using data it collects on users to connect traffickers with potential targets and by electing not to warn users – particularly minors – of the threat of trafficking.[126] Unlike the *Twitter* plaintiffs, the *Facebook* plaintiffs did not allege that the defendant was

[123] *See e.g.*, Doe v. Mark Bates Yahoo!, Inc., No. 5:05-CV-91-DF-CMC, 2006 U.S. Dist. LEXIS 93348, at *12 (E.D. Tex. Dec. 27, 2006) (using Section 230 immunity to dismiss claims against Yahoo! based on its hosting of a group that distributed child pornography); Doe v. Backpage.com, 817 F.3d 12, 22 (1st Cir. 2016) ("We hold that claims that a website facilitates illegal conduct through its posting rules . . . are precluded by section 230(c)(1).").

[124] Herrick v. Grindr LLC, 765 Fed. Appx. 586, 591 (2d Cir. 2019). While *Herrick* was decided after FOSTA was enacted, FOSTA did not apply because the plaintiff did not assert claims under §1595. It is therefore demonstrative of how courts treat claims that a platform's neutral tools facilitated wrongdoing outside the context of FOSTA.

[125] *Id.*

[126] In re Facebook, 625 S.W.3d 80, 97-98 (Tex. 2021).

aware of the specific nature of her interaction with traffickers.[127] Instead, the *Facebook* plaintiffs alleged that Facebook should have been aware of it because sex trafficking is a known problem on Facebook, and because the information was available if Facebook had been looking for it.[128] The Texas Supreme Court affirmed this constructive knowledge theory, finding that by providing its tools without taking steps to prevent them from being used by sex traffickers, Facebook affirmatively participated in a venture with the traffickers.[129] This approach is not universal. The Florida Southern District Court rejected a similar constructive notice claim in *Doe v. Kik Interactive*, where the plaintiff alleged that the defendant messaging platform should have been aware of sex trafficking targeting her because it was aware of other sex trafficking incidents on the platform.[130]

FOSTA remains a relatively unsettled law, with much at stake in its interpretation for companies operating web-based platforms. Some courts have held that FOSTA only applies when the defendant's actions satisfy all elements for criminal conduct under Section 1591, while other courts have held that FOSTA can apply as long as someone involved in the venture is alleged to have acted criminally.[131] As the tide shifts towards expecting companies to take more proactive steps to prevent trafficking and child exploitation on their platforms, *Twitter* and *Facebook* show two

[127] *Id.* at 85. One plaintiff did allege that her mother reported some of the events to Facebook after they occurred, and that Facebook did not respond. *Id.* at 84. The claims at issue, however, were not based on Facebook's failure to respond to these reports. *Id.* at 84.

[128] *Id*.

[129] *Id.* at 97-98. It is worth noting that this was not a finding against Facebook on the merits, but merely a denial of its motion to dismiss where the court considers all allegations in the light most favorable to the plaintiff. Nonetheless, it is significant that these allegations were sufficient to deny Facebook immunity under the FOSTA exemption to §230.

[130] Doe v. Kik Interactive, 482 F. Supp. 3d 1242, 1251 (S.D. Fla. 2020).

[131] *See J.B. v. G6 Hosp., LLC*, No. 19-cv-07848-HSG, 2021 U.S. Dist. LEXIS 240543, at *12 (N.D. Cal. Dec. 16, 2021) ("No court of appeal has ruled on this question to the Court's knowledge, and district courts have reached thoroughly-reasoned but conflicting conclusions."). One year after *J.B.*, the Ninth Circuit held that FOSTA only applies when plaintiffs "plausibly allege that the website's own conduct violated section 1591." *Does v. Reddit*, No. 21-56293, 2022 U.S. App. LEXIS 29510, _ F. 4th _ , at *10 (9th Cir. 2022).

doctrinal pathways through which plaintiffs and courts may pierce the 230 liability shield. The *Twitter* approach to participation in a venture may revitalize distributor liability for interactive service providers and require substantial care in responding to reports of illicit content. The *Facebook* reasoning may further require companies to evaluate how wrongdoers could use their otherwise-neutral tools in furtherance of illicit activities, and to take steps to prevent such uses.

(ii) Liability for role in Content Development

Interactive service providers may also be liable when plaintiffs plead that they had a role in developing the illicit content. Unlike suits where plaintiffs allege that platform hosts are responsible for facilitating harmful actions because those actions were perpetrated on their platforms, in these suits plaintiffs claim that the service provider was itself a content creator. Section 230 protects against suits based on "information provided by another information content provider,"[132] but Section 230 will not apply if the host has a sufficient role in creating the content at issue.[133] Interactive service providers should therefore be careful that any guidance to users is truly neutral such that it does not render them a developer of content.

Courts consider interactive service providers to be content creators or content developers if they materially contribute to the creation of illegal content.[134] This material contribution exists when an entity induces users to create illicit content, but this requires more than a neutral solicitation of content.[135] The platform host must affirmatively induce the illegal nature of the content.[136] For example, in *Fair Housing Council v. Roommates.com*, a website that sought to connect people seeking

---

[132] 42 U.S.C. §230(c)(1) (2018).

[133] Fair Hous. Council v. Roommates.com, 521 F.3d 1157, 1169-70 (9th Cir. 2008).

[134] *Id.*

[135] Jones v. Dirty World Entm't Recordings, 755 F.3d, 416-17 (6th Cir. 2014).

[136] *Id.*

housing and roommates required users to fill out a form in which illegal discriminatory content like preferences regarding sex, sexual orientation, and family status was solicited.[137] The users could not create an account without answering questions soliciting discriminatory preferences.[138] Although the users were ultimately the ones who expressed the discriminatory preferences, the defendant was liable as a developer of the content because it directly solicited the illegal content.[139] Similarly, in *J.S. v. Village Voice Media Holdings*, Backpage – a website where human traffickers posted advertisements of their victims – was liable as a content developer because it designed its content requirements to assist traffickers in posting these advertisements and evading law enforcement.[140] In each of these cases, the defendants had not simply encouraged content creation; their encouragement had directly induced the illegal nature of the content.

By contrast, in *Jones v. Dirty World Entertainment*, the defendant operated a website where he asked users to submit comments and rumors about people.[141] The defendant then selected his favorite comments to post on the website.[142] Under the material contribution test, the defendant was not a developer of defamatory comments he ultimately published because he had not explicitly solicited defamatory content.[143] Merely soliciting content that ends up being illegal or defamatory is not sufficient to incur liability as a content developer.[144]

---

[137] Roommates.com, 521 F.3d at 1161-62.

[138] *Id*.

[139] *Id*. at 1165.

[140] J.S. v. Village Voice Media Holdings, 184 Wn.2d 95, 98 (Wash. 2015).

[141] Jones, 755 F.3d at 402-03.

[142] *Id*.

[143] *Id.* at 416-17.

[144] *Id*.

But the material contribution test is another avenue for courts to work around the Section 230 shield where plaintiffs can plead that platform hosts played a significant role in causing their harms. A recent case, *M.L. v. Craigslist*, demonstrates that a company's recklessness with respect to trafficking content may be sufficient to render it a developer under the material contribution test.[145] In *M.L.*, the plaintiff's allegations primarily focused on actions Craigslist took that relate to all content on its site – not just trafficking-related ads.[146] These allegations included that Craigslist created rules and guidelines for advertisements on its platform, that it designed an anonymous communication system for posters and interested purchasers, and that traffickers paid Craigslist to post on the website's "erotic services" section.[147] The plaintiffs did not allege that Craigslist knew of the specific posts or users at issue, but rather that Craigslist was aware that trafficking occurred on its website and that it had a general relationship with traffickers in which it facilitated their conduct in exchange for payment.[148] Because of the allegations of Craigslist's awareness of trafficking and that Craigslist had an ongoing relationship with the traffickers, Craigslist's content creation guidelines were sufficient to render it a developer and therefore outside the protections of Section 230.[149]

---

[145] M.L. v. Craigslist Inc., No. C19-6153 BHS-TLF, 2020 U.S. Dist. LEXIS 166836, at *33-35 (W.D. Wash. Sep. 11, 2020).

[146] *Id*. at *33-34.

[147] *Id*.

[148] *Id.*

[149] *Id.* at *35. In a later opinion in the same case, the *Craigslist* court dismissed the plaintiff's negligence and strict liability claims against Craigslist, finding that the plaintiff had not sufficiently alleged that Craigslist materially contributed to the content to overcome Section 230 immunity. *M.L. v. Craigslist, Inc.*, No. C19-6153 BHS-TLF, 2022 U.S. Dist. LEXIS 74884, at *47 (W.D. Wash. Apr. 25, 2022). State law claims survived this renewed motion to dismiss. *Id.* While this case does not provide much clarity on the material contribution test, it does demonstrate the litigation risk at issue; Craigslist was required to litigate this case for two years after the first motion to dismiss, only to have some, but not all, claims against it dismissed. *Id*. *See also Doe v. MindGeek USA*, 574 F. Supp. 3d 760, 770-71 (C.D. Cal. 2021) (finding that MindGeek, the operator of Pornhub, was not protected by Section 230 because by categorizing videos using coded language for child pornography and instructing users on how to title videos to

Though these pleadings allege some level of intent on Craigslist's part, it is important to remember that Section 230 decisions are made at the motion to dismiss stage where plaintiffs' allegations are taken as true.[150] Interactive service providers may therefore be at risk of this type of suit alleging content development even when they do not knowingly facilitate trafficking. Although they may successfully avoid liability once all the facts are brought out through discovery and trial, the litigation process involves significant financial and reputational costs.

(iii) In re Facebook: Potential Availability of State Law Claims

One recent case, *In re Facebook*, is of particular note because in it, the Texas Supreme Court permitted state law sex trafficking claims to survive a Section 230 motion to dismiss.[151] It did so purporting to apply current doctrine, using a combination of the developer liability and FOSTA exception theories discussed above.[152] Though there is reason to question the doctrinal soundness of the Texas Court's opinion, it is nonetheless a decision by the highest court in one of the biggest states in the country. The decision demonstrates a strong judicial desire to avoid dismissing sex trafficking claims under Section 230 and is an invitation to claimants to file lawsuits modeled after it in state court.

In *In re Facebook*, plaintiffs were victims of sex trafficking who were identified and recruited by their traffickers on Facebook and Instagram (which is owned by Facebook).[153]After meeting in person, the traffickers posted images of the victims on another platform as advertisements for

---

target people interested in child pornography, MindGeek materially contributed to the illicit content); *Doe #1 v. MG Freesites, Ltd.*, No. 7:21-cv-002200-LSC, 2022 U.S. Dist. LEXIS 21399, at *57 (N.D. Ala. Feb. 9, 2022).

[150] M.L. 2020 U.S. Dist. LEXIS 166836, at *35.

[151] In re Facebook, 625 S.W.3d 80, 101 (Tex. 2021).

[152] *Id*. at 96-101.

[153] *Id.* at 84-85.

prostitution.[154] The plaintiffs sued Facebook under common law theories of negligence, gross-negligence, negligent-undertaking, and products liability.[155] They also asserted claims under a Texas human trafficking statute that mirrors the Federal §1591.[156] Each of these claims was based on the argument that Facebook operated a platform that created an opportunity for human trafficking, thereby putting vulnerable users at risk, and it failed to take sufficient steps to protect users from that risk.[157]

Under traditional Section 230 reasoning, the court dismissed the plaintiffs' common law claims because they "derive[d] from [Facebook's] status … as a 'publisher or speaker'" of the trafficker's content.[158] The court distinguished these common law claims from the state law claims, however, and permitted the state law claims to stand.[159] The court provided two lines of reasoning to support this result.

First, the court stated that unlike the common law claims, the state law claims alleged affirmative conduct on Facebook's part, and that Section 230 does not shield liability for a party's own affirmative acts.[160] For this proposition, the court cites to several cases, all of which were cases in which courts found the defendant to have been a content developer.[161] In *In re Facebook*, however, Facebook was not accused of having developed content, but rather of having taken such affirmative

---

[154] *Id*.

[155] *Id.* at 93.

[156] In re Facebook, at 96.

[157] *Id.* at 85.

[158] *Id.* at 94.

[159] *Id.* at 84-85.

[160] *Id.* at 97.

[161] *In re* Facebook, at 98.

acts as providing a dangerously designed platform and suggesting predatory friends or followers.[162] These actions were previously treated by courts as publisher actions protected by Section 230.[163]

Second, the court held that FOSTA opened the door to state law sex trafficking claims.[164] According to the Texas court, FOSTA did not just carve out federal sex trafficking claims from 230 immunity.[165] Rather, FOSTA was intended as a rule of construction, clarifying that Section 230 was never intended to bar sex trafficking claims like those described in the federal statute.[166] Under this interpretation, FOSTA permits any claims under any statute that is materially similar to the Section 1591 of Title 18.[167] The problem with this is that it is not consistent with the language of FOSTA or Section 230. Pre-FOSTA, Section 230 made no mention of sex trafficking.[168] FOSTA then added to the statute that it shall not be "construed to impair or limit … 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."[169] Though this language creates a specific exception for the federal statute, the Texas court found it permitted claims under any similar sex trafficking statute.

---

[162] *Id.* at 93-94; 97-98.

[163] *See* Herrick v. Grindr, 765 Fed. Appx. 586, 591 (2d Cir. 2019) (holding that Grindr "cannot be held liable for providing 'neutral assistance' in the form of tools and functionality available equally to bad actors and the app's intended users[]").

[164] *In re* Facebook, 625 S.W. 3d at 100-01.

[165] *Id*.

[166] *Id*.

[167] *Id*. Other courts disagree. *But see* A.M. v. Omegle.com, LLC, No. 3:21-cv-01674-MO, 1, 9 (D.Or. 2022) ("The plain text of the statute does not provide a carve out for civil state law trafficking claims."); Doe v. Salesforce.com, No. A1590566, (Cal. Ct. App. 2021) (finding that FOSTA did not permit state law claims for sex trafficking to survive Section 230 defenses).

[168] 42 U.S.C. § 230 (2018).

[169] Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, §2 (2018).

Agree or disagree with the reasoning of *In re Facebook*, it is likely a sign of things to come. With such strong appetite for reconsidering Section 230, other state courts may similarly hold that state law trafficking claims survive Section 230.

(iv) Avenues for Supreme Court Reinterpretation of Section 230

A Supreme Court opinion reinterpreting Section 230 could truly open the floodgates of liability. Because the Supreme Court has never interpreted Section 230, the broad interpretation applied by the *Zeran* court and the other circuits that followed, has been the law of the land.[170] Many of the ways that Section 230 has been applied, however, have been based on expanded readings of the statute, premised on interpreting the policy intent of Congress at the time of enactment.[171] Justice Thomas pointed this out in a recent opinion in which he concurred in the denial of certiorari of *Malwarebytes v. Enigma*, but argued that the Court should seek an appropriate opportunity to evaluate whether the prevailing interpretations of Section 230 are correct.[172] In his *Malwarebytes* concurrence, Thomas criticized these interpretations, writing "Adopting the too-common practice of reading extra immunity into statutes where it does not belong, courts have relied on policy and purpose arguments to grant sweeping protection to Internet platforms."[173] Thomas specifically questioned whether courts properly applied Section 230 to shield defendants from distributor liability and suggested that product defect claims arising from activity on web-based platforms should be outside its protections.[174] The narrower interpretations that Thomas suggested are viable

[170] Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 15-16 (2020) (statement of Thomas, J., respecting denial of certiorari).

[171] *Id.* at 15.

[172] *Id*. at 14.

[173] *Id*. at 15 (internal citations omitted). While Justice Thomas raised four specific areas of concern within Section 230 doctrine, we focus here only on the two that are most relevant to trafficking and child exploitation online.

[174] *Id*. at 15, 17-18.

under the statutory language, and the legal landscape for internet service providers would dramatically change if the Supreme Court were to apply them.

Section 230 can be read as only barring claims that treat interactive service providers as speakers and publishers, while permitting claims that treat them as distributors. The relevant part of the statute reads: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[175] This makes no mention of distributor liability, even though Section 230 was enacted in direct response to *Cubby* and *Stratton Oakmont*, whose outcomes centered on the difference between publisher and distributor liability.[176] The Supreme Court could therefore reject the prevailing approach and hold that only speaker and publisher liability claims are barred by Section 230. Justice Thomas has already vocalized his belief,[177] and considering the widespread support for narrowing 230 immunities, he is likely not alone in holding this perspective.

If distributor liability were revived by a new interpretation of Section 230, web-based platforms could be liable for ensuing harms whenever they host content that they know is illegal, or when they host content that they constructively know is illegal.[178] In the context of hosting online speech, this would raise many difficult questions that would have to be worked out through case law.

With respect to actual knowledge, courts would have to consider questions such as: How sure would companies need to be that the content was illegal? Does any employee's knowledge of

---

[175] 42 U.S.C. § 230(c)(1)(2018).

[176] Malwarebytes Inc., 141 S.Ct. at 14-15; *infra* section 3A (explaining that Section 230 was enacted in response to *Cubby* and *Stratton Oakmont*).

[177] *Malwarebytes Inc.*, 141 S.Ct. at 14-15.

[178] *See Id*. at 14 ("Distributors were thus liable only when they knew (or constructively knew) that content was illegal.").

actionable content suffice to charge the company with knowledge? Is the company charged with knowledge as soon as content is known or reported as illegal, or is time allowed to investigate and remove the content? If so, how much time? Does the answer to these questions change based on the size and/or resources of the company? Does it change based on the number of users of the platform and/or to what extent the disputed content has been and continues to be circulated on the platform?

Constructive knowledge raises potentially thornier questions. Anyone operating online knows – or should know – that there are wrongdoers who could use their platforms for harm. How proactive do service providers need to be in identifying risks? If a company runs a popular photo-sharing platform are they charged with constructive knowledge that because child pornography is widely shared on the internet it must be shared on their platform? Or alternatively, would constructive knowledge be construed more narrowly such that the company could not actively avoid awareness of illicit content, but absent such avoidance is not charged with knowledge?

As discussed above, FOSTA has already revived some elements of distributor liability. FOSTA's impact is limited, however, to trafficking cases where the underlying conduct violates §1591. A reinterpretation of Section 230 that revived distributor liability writ large would have an immediate and significant impact. Companies could be liable for child exploitation claims, for example, particularly those involving child pornography, if plaintiffs can establish that they failed to respond adequately to illegal content posted on their platforms. Indeed, these claims could be brought under common law theories or under any state or federal law.

A reevaluation of Section 230 could also make companies vulnerable to product defect claims that have so far been barred by Section 230. Under current interpretations of 230, courts have dismissed products liability claims like those claiming that companies should be liable because their

products lack necessary safety features or warnings.[179] Though plaintiffs argue that these claims are not based on third-party content but rather on the companies' own actions that enabled the harm, courts consistently describe this as "artful pleading" that seeks to hold internet platforms liable for third-party speech.[180] Under the approach Justice Thomas suggests in *Malwarebytes*, Section 230 immunity would no longer extend to these cases.[181]

This would significantly broaden liability for human trafficking and child exploitation claims, among others. For example, in *Doe v. Myspace*, the plaintiffs argued that their claims were not based on messages that led to the sexual assault of a minor, but on "Myspace's failure to implement basic safety measures to protect minors."[182] The *Herrick v. Grindr* plaintiff based his claims on Grindr's lack of safety features preventing its geolocation feature from being used for harassment and preventing false impersonating accounts.[183] The *Kik Interactive* plaintiff alleged that Kik facilitated child exploitation by not implementing policies sufficient to combat it.[184] In each of these cases, courts dismissed these product liability claims under Section 230's immunity, citing cases that

---

[179] *See, e.g.*, Herrick v. Grindr, 765 Fed. Appx. 586, 590-91 (2d Cir. 2019)*; see also* Doe v. Kik Interactive, 482 F. Supp. 3d 1242, 1250-51 (S.D. Fla. 2020).

[180] *See, e.g.*, In re Facebook, 625 S.W.3d 80, 90 (Tex. 2021) ("[A] plaintiff in a state tort lawsuit cannot circumvent section 230 through 'artful pleading' if his 'allegations are merely another way of claiming that [a defendant] was liable' for harms occasioned by 'third-party-generated content' on its website." (quoting Doe v. Myspace, 528 F.3d 413, 420 (5th Cir. 2008)).

[181] Malwarebytes Inc., 141 S.Ct. at 18. One court has already taken this approach, permitting a products liability claim to survive a motion to dismiss where the defendant-company hosted anonymous chat rooms that ultimately connected a young girl with an adul. *See* A.M. v. Omegle.com, LLC, No. 3:21-cv-01674-MO, 2022 U.S. Dist. LEXIS 123695, at *11-12 (D. Oreg., Jul. 13, 2022) ("Plaintiff's case does not rest on third party content. Plaintiff's contention is that the product is designed in a way that connects ind. Another case involving the same defendant and materially identical claims, however, was dismissed. *See* M.H. v. Omegle.com, LLC, No. 8:21-cv-814-VMC-TGW, 2022 U.S. Dist. LEXIS 4543, at *14 (M.D. Fla. Jan. 10, 2022) ("The CDA bars such claims as they seek to redirect liability onto [the defendant' for the ultimate actions of their users.").

[182] Myspace, 528 F.3d at 419.

[183] Herrick, 765 Fed. Appx. at 590.

[184] Doe v. Kik Interactive, 482 F. Supp. 3d 1242, 1245 (S.D. Fla. 2020).

interpret 230 to bar any claim where the underlying harm was caused by content produced by a third-party.[185]

Like the reintroduction of distributor liability for internet-based harms, newly permitted products liability claims would open a host of new legal issues for courts to evaluate. Traditional tort principles of negligence would have to be reimagined for the social media world. What level of care is appropriate on a platform that is open to anyone with internet access? What duty follows when companies target their services to minors? With the known presence of human trafficking and child exploitation online, how much risk is acceptable, and what level of safety must companies ensure to successfully defend against negligence claims? Section 230 immunity has largely prevented courts from answering these questions to date. But basic tort principles support the proposition that companies owe a duty of care to users for foreseeable harms.[186] If Section 230 immunity is narrowed or eliminated entirely, companies would need to carefully evaluate the risks their products create and what obligations they may have to mitigate them.

These interpretive changes are both plausible and doctrinally viable. Some of them may result from the Supreme Court's forthcoming review of *Gonzalez v. Google*, which it will hear in its 2023 term.[187] In *Gonzalez*, the plaintiffs sued Google, as the owner of YouTube, for its role in promoting the spread of ISIS recruiting materials.[188] Plaintiffs, family members of a victim killed in terrorist attacks, alleged that the defendant's platform not only allowed ISIS to post videos that

---

[185] *See* Myspace, 528 F.3d at 420 ("Their allegations are merely another way of claiming that Myspace was liable for publishing the communications . . . ."); *Grindr*, 765 Fed. Appx. at 590 (granting motion to dismiss because the "claims are based on information provided by another information content provider . . . ."); Kik Interactive, 482 F. Supp. 3d at 1249 (stating that the plaintiff's unsafe product claims were "exactly the type of claim that CDA immunity bars.").

[186] *See* Louis R. Frumer & Melvin I. Friedman, *Products Liability* §2.02 (Matthew Bender, Rev. Ed. 2021).

[187] Gonzalez v. Google, 214 L. Ed 2d 12 (S. Ct. 2022)

[188] Gonzalez v. Google, 2 F.4th 871, 880-81 (9th Cir. 2021).

would radicalize recruits and further its mission, but that it affirmatively supported the spread of ISIS content.[189] These allegations were based on a number of features, including algorithms that recommended content based on viewing history, assistance with search terms, the pairing of advertisements with videos, and profit sharing with content creators.[190] The trial court held that all but the profit-sharing claims were barred by Section 230.[191] The Ninth Circuit affirmed consistent with longstanding precedent and in spite of hesitation about the validity of that precedent as expressed by a concurrence.[192]

With *Gonzalez*, the Supreme Court has the opportunity to entirely reshape Section 230 doctrine. The Ninth Circuit held that Google could not be held liable for its algorithms' promotion of ISIS content because "the algorithms do not treat ISIS-created content differently than any other third-party created content[.]"[193] A Supreme Court opinion rejecting this conclusion could create a standard of care that platform hosts would need to meet to ensure that their algorithms are not promoting improper content. Further, *Gonzalez* presents an opportunity for the Court to weigh in on the material contribution test, which the Ninth Circuit applied to find that pairing ISIS-created content with advertising and other videos in a "mosaic" format did not render Google a content creator.[194] The Court could craft a new standard for determining when a platform host is actually creating or contributing to the creation of content. Finally, *Gonzalez* gives the Court the opportunity

[189] *Id*.

[190] *Id*.

[191] *Id*.

[192] *Id*. at 914.

[193] *Id*. at 894.

[194] *Id*. at 894-95.

to more broadly evaluate Section 230's scope. The Court could challenge interpretations as far back as *Zeran*, and completely redefine the contours of the Section 230 defense.

(v) Proposed Legislative Changes

Changes to Section 230 immunity may also come from the legislative branch. Proposals have been advanced suggesting an immense range of policy solutions.[195] While it is difficult to predict what legislation will pass, common trends among the proposals suggest the types of policies that may be advanced in the foreseeable future.

One notable proposal was offered by the Department of Justice in 2020. DOJ conducted an expansive review of Section 230's impact through a public workshop, expert roundtable, written submissions, and industry listening sessions.[196] After this review, DOJ proposed a series of amendments to Section 230 based on the recommendations from stakeholders. Under those proposed amendments, companies whose platforms are used to facilitate human trafficking and child exploitation would be open to liability in ways that have been traditionally protected by Section 230. These amendments include new FOSTA-like carve-outs for child abuse and cyberstalking, as well as carve-outs for cases when platforms have notice or actual knowledge that content is unlawful.[197] The DOJ proposal would also prevent companies from using 230 as a shield against civil suits brought by the federal government.[198] Finally, the DOJ recommended a "Bad Samaritan" carve-out that would deny Section 230 immunity to anyone who intentionally promotes or facilitates

[195] *See* Congressional Research Service, Section 230: An Overview, Apr. 7, 2021, at 30 (https://crsreports.congress.gov/product/pdf/R/R46751) ("Twenty-six bills in the 116th Congress would have amended Section 230.").

[196] U.S. DEP'T OF JUST., SECTION 230 – NURTURING INNOVATION OR FOSTERING UNACCOUNTABILITY? KEY TAKEAWAYS AND RECOMMENDATIONS, 7 (2020).

[197] U.S. DEP'T OF JUST, supra note 70 at 3.

[198] *Id.*

wrongful conduct.[199] Together, these amendments would create significant exposure to companies operating web-based platforms and do not take reasonable steps to prevent the use of their sites for human trafficking and child exploitation.

The child sex abuse and cyberstalking carve-outs in the DOJ proposal go a step further than FOSTA by creating an affirmative duty to take reasonable steps to address risks. Unlike FOSTA, which requires that plaintiffs show that the defendant participated in a venture with traffickers, this DOJ proposal would apply a tort-based standard of due care.[200] Companies would have an obligation to take reasonable steps to address foreseeable risks, rather than merely avoiding action that constitutes participation in a venture with wrongdoers.

Many of the proposals that have been brought to Congress mirror the 2020 DOJ proposal. For example, the bipartisan EARN IT Act would create a carve-out to permit liability for platforms that host child sexual abuse materials.[201] The PACT Act would eliminate Section 230 immunity for platforms that fail to remove illegal content within a certain time period after being notified of the content's existence.[202] Proposals - including the CASE-IT Act and Stopping Big Tech's Censorship Act - also condition Section 230 immunity on organizations implementing appropriate safeguards against illicit uses of their platforms.[203]

Several proposals have focused on the role of algorithms and advertisements in recommending content. The Justice Against Malicious Algorithms Act, for example, would permit

---

[199] *Id*. (The 2020 DOJ proposal includes a number of other changes to Section 230. This article's scope is limited to those proposals that would affect liability for human trafficking and child exploitation, so we are not addressing all elements of the DOJ's recommendations. It is worth noting that the proposal also includes a recommendation that 230 be amended to clarify that it does not grant immunity in any civil action brought by the federal government.).

[201] EARN IT Act of 2020, S. 3398, 116th Cong. §5 (2020).

[202] PACT Act., S. 4066, 116th Cong. §6 (2020).

[203] CASE-IT Act, H.R. 8719, 116th Cong., §2 (2020); Stopping Big Tech's Censorship Act, S. 4062, 116th Cong. §2 (2020).

platform hosts to be liable when recommendations provided by their algorithms "materially contribute[] to a physical or severe emotional injury."[204] Proposals like this are designed to address situations where plaintiffs are alleged to have been introduced to their traffickers as a result of algorithms learning the preferences of the wrongdoers. This would further erode – and in some cases entirely eliminate – the "neutral tools" argument that many entities have relied on in avoiding liability for the abuse of their platforms' features.

Most proposals fall short of the full repeal of Section 230 that some have suggested, but for companies whose platforms might be used by individuals engaged in human trafficking, child exploitation, or other covered misconduct, any of these changes could present significant legal risks. New FOSTA-like carve-outs would require that any company whose platform creates foreseeable opportunities for this type of abuse take affirmative steps to improve safety and prevent their products from being used in nefarious ways. Given the broad (albeit shrinking) immunity provided by the current Section 230 doctrine, this would be a significant shift.

4. **Conclusion**

There are reasons beyond legal liability that entities operating online should take steps to make users on their platforms safe from trafficking and child exploitation. As these problems continue to grow, a defense that an entity did not intend for its platform to be abused in this way will not be enough to avoid certain forms of accountability. It is becoming increasingly evident that not only *can* predators use interactive online spaces to entrap victims, but that they will.

Platform hosts should be thoughtful about what risks exist in their online environments, and what steps they are taking to address them. Considering the mounting evidence that not only are these problems significant, but that they can be prevented in some instances, failing to act may not

[204] Justice Against Malicious Algorithms Act, H.R. 5596, 117th Cong. §2 (2021).

be seen as neutrality; instead it can be viewed as acquiescing to known dangers.[205] The changes discussed in this article demonstrate the legal system's shift in that direction. And legislators are seeking to hold tech companies responsible for taking reasonable steps to reduce known risks. Beyond liability and legislative pressure, consumers will come to expect positive action. With the growth of Environmental, Social, and Governance (ESG) investing, investors are looking at more than a company's bottom line.[206] Whether a company acts to protect their users from child exploitation and trafficking may well affect how it is evaluated by investors.[207] And as the Section 230 liability shield shrinks, details of how these harms occur on platforms will be further revealed through the litigation process. Companies hesitant to act risk not only financial liability, but severe reputational harm. On the other hand, those who take proactive steps now have the opportunity to not only minimize those risks, but to act as leaders on an issue vital to the safety of our communities.

[205] *See* Brian Bushard, *Pornhub CEO and COO Resign Amid Blowback Over nonconsensual Videos of Minors*, Forbes (Jul. 21, 2022) (https://www.forbes.com/sites/brianbushard/2022/06/21/pornhub-ceo-and-coo-resign-amid-blowback-over-nonconsensual-videos-of-minors/amp/). (Evidence of this shift in public sentiment can be found in the recent resignations of MindGeek's CEO and COO. While Pornhub has been accused of hosting illicit content (including child pornography) a number of times – including in cases discussed above – recent publicity relating to its hosting of nonconsensual videos forced key leadership to resign.).

[206] *See* E. Napoletano & Benjamin Curry, Environmental, Social and Governance: What is ESG Investing?, Forbes (Mar. 1, 2021) (https://www.forbes.com/advisor/investing/esg-investing/).

[207] *See, e.g.*, Alicia Adamczyk, Your ESG Fund Might be Invested in Facebook – and it Highlights a Major Issue with Sustainable Investing, cnbc.com (Oct. 26, 2021)(https://www.cnbc.com/2021/10/26/your-esg-fund-might-be-invested-in-facebook.html) (noting that Facebook is used for sex trafficking, and that ESG funds' investment in the company undermines the premise of ESG investing).