

# Skirting Liability for Child Sexual Material

# Abuse Online

Understand how tech companies are using a statute aimed at protecting children online to evade liability for the spread of child sexual abuse material.

By || **MARGARET MABIE**

The internet allows images and videos of recorded child sexual abuse to spread prolifically around the world at warp speed. This child sexual abuse material (CSAM) is a digital crime scene that follows its victims as they grow up and repeatedly revictimizes them.<sup>1</sup> New abusers trade CSAM throughout the victim's life—and even after their death. Victims can face millions of dollars in losses and damages across their lifetime in medical costs, lost wages, pain and suffering, and other harms related to the uncontrolled circulation of their CSAM online.<sup>2</sup>

In 2022, the National Center for Missing and Exploited Children received over 32.5 million reports of CSAM.<sup>3</sup> And since 2017, Project Arachnid—a tool created and operated by the Canadian Centre for Child Protection—processed more than 100 billion images of CSAM and sent out millions of notices to tech companies requesting removal of CSAM hosted on their platforms.<sup>4</sup>

The Canadian Centre for Child Protection used Project Arachnid to determine that the tech companies they observed knew of 48% of all media by the time they received a takedown notice.<sup>5</sup> So much of this material exists on the internet because children are easily accessible through social media and can be sexually violated without a predator ever putting their hands on the child.<sup>6</sup>

Tech companies now operate with impunity due to outdated legislation designed for an internet that no longer exists. The tools to detect and remove CSAM exist, but tech companies have failed to efficiently use these tools to stop the spread of it online. For example, PhotoDNA technology can help detect, disrupt, and report the distribution of CSAM and child exploitation material.<sup>7</sup> The internet today is more dangerous

than ever, but civil litigation can serve as a formidable tool to protect children.

### Section 230 and the Publisher Immunity Problem

While child sexual abuse has been a crime for centuries, possessing material depicting such abuse was not necessarily criminalized until the Protection of Children from Sexual Exploitation Act in 1977.<sup>8</sup> And until the early 1980s, it was often seen as a “victimless crime”—children depicted in abusive content were largely invisible to the courts.

Forty years ago *New York v. Ferber*, a case involving a New York bookstore owner's distribution of third-party illegal content, illustrated that the marketplace for CSAM must be eradicated on all fronts.<sup>9</sup> In that case, the U.S. Supreme Court recognized the grave “physiological, emotional, and mental” injuries suffered by victims of child pornography.<sup>10</sup> Victims of CSAM face at least two distinct harms: first, the child sexual abuse committed against them and second, the memorialization and uncontrolled circulation of that abuse.

The Court in *Ferber* explained that the victim must “go through life knowing that the recording is circulating within the mass distribution system for child pornography.”<sup>11</sup> Following the reasoning in *Ferber*, as digital publishing developed in the early 1990s, tech companies were held liable for libelous content in their editorial role as publishers.<sup>12</sup>

On Feb. 8, 1996, Congress passed §230 of the Communications Decency Act (CDA).<sup>13</sup> Section 230 was originally passed with a goal of “family empowerment”<sup>14</sup> but turned into an unprecedented immunity clause empowering one private industry. Shortly after its passage, the Fourth Circuit held that §230 barred all claims for “distributor” liability against an

internet “publisher” of defamatory statements.<sup>15</sup>

Next, the Supreme Court stripped §230 of the power to protect kids and empower families, and there was nothing decent about it.<sup>16</sup> The Court found in *Reno v. American Civil Liberties Union* that the statute's insufficiently narrow use of “‘indecent transmission’ and ‘patently offensive display’” provisions abridged “freedom of speech” in violation of the First Amendment.<sup>17</sup> What was left after the *Reno* court struck the original child protection provisions from §230 were two immunity provisions: §230(c)(1) and (c)(2).<sup>18</sup>

These two immunity provisions serve as hurdles that advocates for victims must surpass. Section 230(c)(1) provides internet companies with publishers' immunity for third-party content—it specifies that service providers may not be treated as “the publisher or speaker of any information provided by another information content provider.”<sup>19</sup> Section 230(c)(2) provides for “good Samaritan” immunity to internet companies for voluntarily acting to “restrict access” to objectionable material.<sup>20</sup>

The decision in *Reno* transformed §230 from a sword for child victims of injustice to a shield of impunity for internet companies. So despite efforts to hold tech companies accountable for the spread of CSAM, §230 actually stands in the way of accountability.

*Reno* was decided early on in the development of the tech industry—when a very different internet from the one we now know existed. But to add insult to the injuries of *Reno*, in 2002, the Supreme Court in *Ashcroft v. Free Speech Coalition* held that the Child Pornography Prevention Act's ban on “virtual child pornography” that did not depict “real minors” was “overbroad and unconstitutional.”<sup>21</sup>

The Tenth Circuit then held that “juries are still capable of distinguishing

between real and virtual images.”<sup>22</sup> The Eighth Circuit held that juries are able to deduce the authenticity of images of CSAM.<sup>23</sup> Similarly, the Fifth and Sixth Circuits held that a jury could determine whether an image depicts real children.<sup>24</sup> But the Sixth Circuit determined that morphed child pornography using any depictions of real minors does constitute illegal CSAM.<sup>25</sup>

Recent technological advancements in artificial intelligence may put these post-*Ashcroft* circuit court holdings to the test as this technology can “be used to produce new online child sexual abuse material from already existing material.”<sup>26</sup> Today’s children are at extreme risk of harm from computer-generated CSAM, sextortion, deep fakes, online luring, and other serious digital harms related to the creation of sexually explicit material which can result in lifelong trauma and victimization.<sup>27</sup> Parents and advocates are fighting an uphill battle to protect kids online, now against some of the largest companies in the world.

### Where Do We Go Next?

Section 230(c) is titled “Protection For ‘Good Samaritan’ Blocking and Screening of Offensive Material” and the substance “can and should be interpreted consistent with its caption.”<sup>28</sup> It is clear that “when Congress passed Section 230 it didn’t intend to prevent the enforcement of all laws online.”<sup>29</sup>

In this regard, the Tenth Circuit has held that §230 did not immunize defendants from their illegal conduct when they “solicited requests” for information, “paid researchers to find it, [and] knew that the researchers were likely to use improper methods.”<sup>30</sup> The court reasoned that the defendants’ “actions were not ‘neutral’ with respect to generating offensive content; on the contrary, its actions were intended to generate such content” because they solicited and purchased research that

they knew or should have known would be improper or illegal.<sup>31</sup>

**Exceptions under 18 U.S.C. §1591 and §1595.** In the days of print newspapers, Backpage served as a classified advertising section—but when this section went digital it became a hub for sex trafficking and child sexual abuse.<sup>32</sup> The early cases against Backpage were a driving force in the 2018 Fight Online Sex Trafficking Act and the Stop Enabling Sex Traffickers Act of 2018 (FOSTA-SESTA).<sup>33</sup>

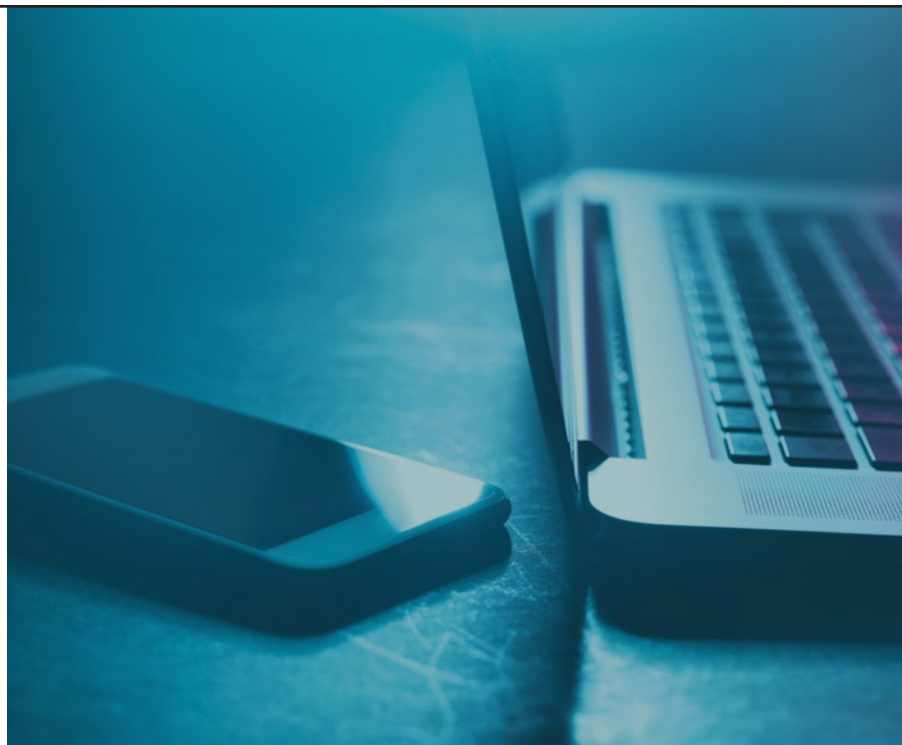
In the *Backpage* cases, the First Circuit ruled that §230 barred CSAM victims’ claims—that is, until two district courts subsequently refused to dismiss similarly situated claims on §230 grounds due to evidence that the internet company had contributed to the development of the illegal content at issue.<sup>34</sup>

Congress, recognizing that sex trafficking markets flourished online, materially limited §230’s immunity with FOSTA-SESTA to provide exceptions to immunity for claims brought by victims

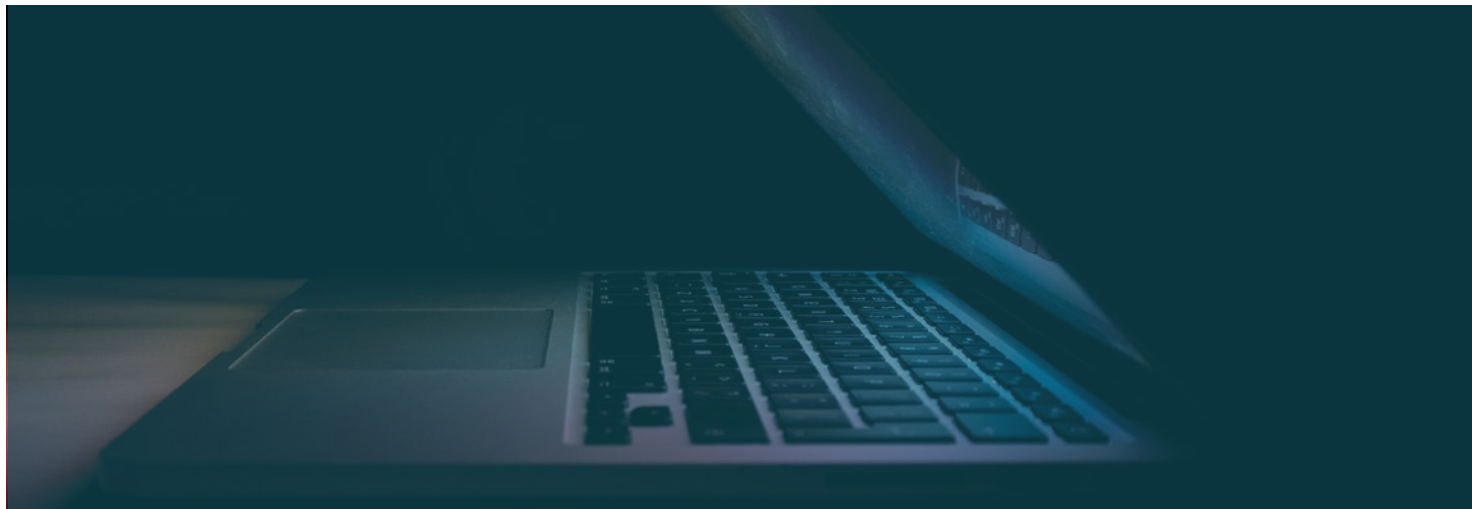
of sex trafficking against websites that benefitted from sexual abuse. Congress sought to clarify that immunity protections were not intended to protect sex traffickers nor those that profit from sex trafficking.<sup>35</sup>

And courts have held that victims seeking civil remedies, as provided for under §1595, do not require the same proof of knowledge as is required under §1591, which criminalizes sex trafficking, because the “language of §1591 differs from the language of §1595” in that “the former does not have a constructive knowledge element manifested by ‘should have known’ language.”<sup>36</sup>

CSAM is often created on demand or used to advertise for hands-on child sexual abuse, allowing predators to preview their abuse. Sex trafficking victims and victims of CSAM may use the civil remedies under 18 U.S.C. §1595 against perpetrators of trafficking and those who knowingly benefit financially from a sex trafficking venture.<sup>37</sup> While courts differ in interpreting the



**The tools to detect and remove CSAM exist, but tech companies have failed to efficiently use them.**



## Congress has sought to clarify that §230 immunity protections were not intended to protect sex traffickers nor those that profit from sex trafficking.

applicable mens rea standards, direct liability and beneficiary liability for sex trafficking are statutorily excepted from §230 immunity.<sup>38</sup>

Beneficiary liability is especially crucial in that internet companies profit from the sales and engagement of sex traffickers using their platforms in ways that may mean they “took part in a common undertaking or enterprise involving risk and potential profit.”<sup>39</sup> Tech companies may continue to take a head-in-the-sand approach to CSAM detection and removal, but the industry does so at its own peril. This approach may in fact reveal consciousness of guilt and help plaintiffs prove that companies knew or should have known of the abuse.<sup>40</sup> Courts have held that “knowledge through deliberate indifference occurs where a party acts with an awareness of the high probability of the existence of the fact in question.”<sup>41</sup>

**Exemptions under 18 U.S.C. §2252, §2252A, and §2255.** CSAM is not protected speech.<sup>42</sup> Specifically, courts have found that “child pornography is not lawful ‘information provided by

another information content provider’ as contemplated by Section 230. . . . Rather, it is illegal contraband, stemming from the sexual abuse of a child, beyond the covering of First Amendment protection.”<sup>43</sup>

Additionally, courts have held that CSAM is “outside any other protection or immunity under the law, including Section 230,” which “has ‘no effect on criminal law’”—including 18 U.S.C. §2252 and §2252A, statutes that criminalize activities related to CSAM such as its possession and distribution.<sup>44</sup> And the Supreme Court has gone on to hold that “everyone who reproduces, distributes, or possesses the images of the victim’s abuse . . . plays a part in sustaining and aggravating this tragedy.”<sup>45</sup> That includes the tech companies and their executives that fail to stop the spread of the material on their online platforms.<sup>46</sup>

Passed as part of the Child Abuse Victims’ Rights Act of 1986 and amended in 2005, 18 U.S.C. §2255 (Masha’s Law) “empowers victims of child sexual abuse to recover money for the harms caused by their abusers”—and this is not limited to criminal offenders. Masha’s

Law operates as a civil remedy for violations of §§2252, 2252A, and other predicate acts.<sup>47</sup> An actual “criminal conviction is not necessary for [a] Defendant to face civil liability for the underlying acts.”<sup>48</sup>

Masha’s Law provides victims depicted in CSAM with an option to seek liquidated damages as a statutory right, meaning these plaintiffs can often avoid depositions or extensive discovery by limiting the damages they seek.<sup>49</sup> CSAM is “like a defamatory statement,” child abuse images and video repeatedly violate a victim’s privacy and injure a victim’s reputation and emotional well-being.<sup>50</sup>

### Recent Developments on §230

The Ninth Circuit in *Lemmon v. Snap* recently held that §230 did not bar products liability claims against Snapchat for its speed filters because the defendants’ defective and unsafe product design and architecture caused the plaintiff’s harm and implicated Snap’s own actions.<sup>51</sup>

Products liability claims against a website with the tagline “talk to

strangers” recently prevailed in Oregon district court, which refused to apply §230 immunity to claims involving the spread of CSAM when an internet platform was “designed [in] a way that connects individuals who should not be connected.”<sup>52</sup>


And the Ninth Circuit found in *Gonzales v. Google* that “Section 230’s sweeping immunity is likely premised on an antiquated understanding of the extent to which it is possible to screen content posted by third parties.”<sup>53</sup> The Ninth Circuit also held that courts must be cautious to not exceed the purview of §230 immunity and that the CDA does not bar a failure-to-warn claim.<sup>54</sup> The Supreme Court, however, declined in May 2023 to determine the scope of §230 immunity in *Gonzales*.<sup>55</sup>

Products liability cases are continuing to chip away at §230 immunity. Parents and young adults are now bringing personal injury claims for defective design, failure to warn, negligence, fraudulent concealment, negligent misrepresentation, wrongful death, survival actions, loss of consortium, and violations of 18 U.S.C. §§1595, 2255, 2252A(f), 2258B and other statutes on behalf of minor victims of Meta, Snap, TikTok, and YouTube. These claims have been consolidated in a multidistrict litigation in the Northern District of California and in a Judicial Council Coordination Proceeding in California state court.<sup>56</sup> In October in the California state court proceeding, the court held in a landmark decision that the plaintiffs’ state law claims for general negligence and fraudulent concealment were not barred by §230 because those claims implicate the defendants’ design features.<sup>57</sup>

While supervision apps<sup>58</sup> exist and can be useful tools for parents to help monitor kids’ online activities, no amount of supervision replaces the need for tech companies to implement

## AAJ RESOURCES

- CDA Section 230 Litigation Group
- Child Sex Abuse Litigation Group
- Child Sexual Abuse Litigation Webinar: “Journey to Justice”

safety-by-design principles and prioritize child protection. Plaintiff lawyers challenging §230 immunity are beginning to force social media companies and their financial lenders out of a long-lived state of complacency. The internet that exists today may be harmful, but accountability and redress are coming soon to a theater near you. 



**Margaret Mabie** is a partner at Marsh Law in New York City and can be reached at [margaret.mabie@marsh.law](mailto:margaret.mabie@marsh.law).

**NOTES**

1. For detailed definitions, see 18 U.S.C. §2256 (2018).
2. U.N. Off. on Drugs & Crime, *Towards Zero: An Initiative to Reduce the Availability of Child Sexual Abuse Material on the Internet*, June 26–27, 2023, at 22, [https://www.unodc.org/pdf/criminal\\_justice/endVAC/EGM/EGM\\_CSAM\\_Removal\\_Background\\_Paper.pdf](https://www.unodc.org/pdf/criminal_justice/endVAC/EGM/EGM_CSAM_Removal_Background_Paper.pdf).
3. Nat’l Ctr. for Missing & Exploited Child. (NCMEC), *CyberTipline Data 2022 Report*, <https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata>.
4. Can. Ctr. for Child Prot., *Global Tool Disrupting International Distribution of Child Sexual Abuse Imagery Marks Five Years*, Jan. 17, 2022, [https://protectchildren.ca/en/press-and-media/news-releases/2022/project-arachnid\\_5year](https://protectchildren.ca/en/press-and-media/news-releases/2022/project-arachnid_5year).
5. Can. Ctr. for Child Prot., *2020–2021 Social Value Report*, 2022, at 5, [https://www.protectchildren.ca/pdfs/C3P\\_SocialValueReport\\_2020-2021\\_en.pdf](https://www.protectchildren.ca/pdfs/C3P_SocialValueReport_2020-2021_en.pdf).
6. Rachel Haney, *When “Safe at Home” Is Not Safe: Addressing the Increase of Online Child Sexual Abuse in the Covid-19 Pandemic*, SciTech Law, Summer 2021, at 22, 26 (“Evidence also shows an increase in self-generated CSAM as more online time has allowed greater opportunities for

- perpetrators to groom and exploit children.”); Brenna O’Donnell, *COVID-19 and Missing & Exploited Children*, NCMEC Blog, Apr. 30, 2021, <https://www.missingkids.org/blog/2020/covid-19-and-missing-and-exploited-children>.
7. Hany Farid, *Reining in Online Abuses*, 19 Tech. & Innovation, 593, 595–96 (2018). PhotoDNA is not facial recognition software and cannot be used to identify a person or object; rather, it’s designed to scan for known CSAM using unique digital signatures and has a one-in-50-billion false positivity rate. See Can. Ctr. for Child Prot., *Detecting CSA Online: A Technical and Historical Primer for Policy Makers*, 2023, <https://www.protectchildren.ca/en/resources-research/hany-farid-photodna/>.
  8. 18 U.S.C. §§2251–2260a; see also U.S. Sent’g Comm’n, *The History of Child Pornography Guidelines*, 8–9, Oct. 2009, [https://www.uscc.gov/sites/default/files/pdf/research-and-publications/research-projects-and-surveys/sex-offenses/20091030\\_History\\_Child\\_Pornography\\_Guidelines.pdf](https://www.uscc.gov/sites/default/files/pdf/research-and-publications/research-projects-and-surveys/sex-offenses/20091030_History_Child_Pornography_Guidelines.pdf).
  9. *New York v. Ferber*, 458 U.S. 747, 758 (1982).
  10. *Id.*
  11. *Id.* at 759, n. 10, 751–52. The defendant in *Ferber* was a bookstore owner convicted under a New York statute prohibiting the promotion of a sexual performance by a child and distributing material depicting such a performance.
  12. *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710, at \*7 (N.Y. Sup. Ct. May 24, 1995).
  13. See 47 U.S.C. §230 (1994 ed., Supp. II); 141 Cong. Rec. 27881 (1995).
  14. See Mary Graw Leary, *History Repeats Itself: Some New Faces Behind Sex Trafficking Are More Familiar Than You Think*, 68 Emory L.J. Online 1083, 1108, 1087 (2019) (citing S. Rep. No. 104–23, at 59 (1995)) (“The information superhighway should be safe for families and children. . . . The decency provisions increase the penalties for obscene, indecent, harassing or other wrongful uses of telecommunications facilities; protect privacy; protect families from uninvited or unwanted cable programming which is unsuitable for children and give cable operators authority to refuse to transmit programs or portions of programs on public or leased access channels which contain obscenity, indecency, or nudity.”).
  15. *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 331–33 (4th Cir. 1997).
  16. *Reno v. ACLU*, 521 U.S. 844, 882 (1997).
  17. *Id.* at 849, 858.
  18. See 47 U.S.C.A. §223 (1994 ed., Supp. II); 47 U.S.C. §230.
  19. 47 U.S.C. §230(c)(1).

20. 47 U.S.C. §230(c)(2).
21. *Ashcroft v. Free Speech Coalition*, 535 U.S. 234, 256–58 (2002); see also *United States v. Hilton*, 386 F.3d 13, 14 (1st Cir. 2004) (“new photographic and computer imaging technologies make it possible to produce by electronic, mechanical, or other means, visual depictions of what appear to be children engaging in sexually explicit conduct that are virtually indistinguishable to the unsuspecting viewer from unretouched photographic images of actual children.”) (citing Child Pornography Prevention Act of 1996, Pub. L. No. 104–208, div. A, tit. I, §121(1)(5), 110 Stat. 3009–26 (1996)).
22. *United States v. Kimler*, 335 F.3d 1132, 1142 (10th Cir. 2003).
23. *United States v. Deaton*, 328 F.3d 454, 455–56 (8th Cir. 2003).
24. *United States v. Farrelly*, 389 F.3d 649, 655 (6th Cir. 2004); *United States v. Slanina*, 369 F.3d 356, 357 (5th Cir. 2004).
25. *Doe v. Boland*, 698 F.3d 877, 880 (6th Cir. 2012).
26. NetClean, NetClean Report 2018, at 34, <https://tinyurl.com/bdtza94p>; see also Abigail Olson, *The Double-Side of Deepfakes: Obstacles and Assets in the Fight Against Child Pornography*, 56 Ga. L. Rev. 865, 876 (2022).
27. *Id.*
28. *Doe v. GTE Corp.*, 347 F.3d 655, 660 (7th Cir. 2003).
29. *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1175 (9th Cir. 2008) (holding that §230 did not apply to unlawful acts of website operators nor to websites designed to promote unlawful behavior).
30. *FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1200–01 (10th Cir. 2009).
31. *Id.* at 1201.
32. See *Jane Doe No. 1 v. Backpage.com, LLC*, 817 F.3d 12, 17 (1st Cir. 2016); *Fla. Abolitionist v. Backpage.com, LLC*, 2018 WL 1587477, at \*4–5 (M.D. Fla. Mar. 31, 2018); *Doe No. 1 v. Backpage.com, LLC*, 2018 WL 1542056, at \*2 (D. Mass. Mar. 29, 2018).
33. Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 1115-164, 132 Stat. 1253 (codified as amended in scattered sections of 18 and 47 U.S.C.) (2018).
34. *Jane Doe No. 1*, 817 F.3d at 22; *Fla. Abolitionist*, 2018 WL 1587477, at \*5; *Doe No. 1*, 2018 WL 1542056, at \*1.
35. Compare Telecommunications Act of 1996 §230, Pub. L. 104-104, 110 Stat. 137 (1996) with Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 1115-164, 132 Stat. 1253 (2018) (codified as amended in scattered sections of 18 and 47 U.S.C.).
36. *Doe v. Red Roof Inns Inc.*, 21 F.4th 714, 719 (11th Cir. 2021); *S.Y. v. Naples Hotel Co.*, 376 F. Supp. 3d 1251, 1256 (M.D. Fla. 2020); *M.A. v. Wyndham Hotels & Resorts, Inc.*, 425 F. Supp. 3d 959, 969 (S.D. Ohio 2019).
37. *Doe #1 v. MG Freesites, Ltd.*, 2022 WL 407147, at \*12 (N.D. Ala. Feb. 9, 2022) (noting that 18 U.S.C. §1595(a) allows “sex trafficking victims to bring civil claims against ‘whoever knowingly benefits, financially or by receiving anything of value from participation in a venture which that person knew or should have known has engaged in an act in violation of this chapter’”).

38. *See Does 1-6 v. Reddit, Inc.*, 51 F.4th 1137, 1140–41 (9th Cir. 2022), *cert. denied sub nom.*, 143 S. Ct. 2560 (U.S. 2023); *Doe v. Mindgeek USA, Inc.*, 558 F. Supp. 828, 835 (C.D. Cal. 2021).
39. *Red Roof Inns, Inc.*, 21 F.4th at 725.
40. *G.G. v. Salesforce.com, Inc.*, 76 F.4th 544, 557 (7th Cir. 2023) (“By way of analogy, a taxi service transporting trafficking victims on behalf of traffickers could claim that it lacked constructive knowledge where it knew that it was generally transporting trafficking victims so long as the drivers were shielded from seeing who specifically was in the back of their taxis. Or consider a prostitution ring that hires a construction company to build a better brothel, one that attracts more customers and is better insulated from the prying eyes of law enforcement. The contractor knows that the business is generally engaged in sex trafficking, but so long as the contractor does not know of any individual victim, it would be insulated from civil liability. In other words, the larger the sex-trafficking venture, the less likely a victim would be able to prove sufficient knowledge. Nothing in the statutory text requires such an odd result.”); *see also Jane Doe 1 v. Deutsche Bank Aktiengesellschaft*, 2023 WL 3167633, at \*10–11 (S.D.N.Y. May 1, 2023); *Jane Doe 1 v. JP Morgan Chase Bank, N.A.*, 2023 WL 2871092, at \* 10 (S.D.N.Y. Apr. 10, 2023); *Fleites v. Mindgeek S.A.R.L.*, 617 F. Supp. 3d 1146, 1161 (C.D. Cal. 2022).
41. *Tilton v. Playboy Entm’t Grp, Inc.*, 554 F.3d 1371, 1378 (11th Cir. 2009) (quoting *United States v. Hristov*, 466 F.3d 949, 952 (11th Cir. 2006)). Financial institutions also are facing increasing accountability measures alongside tech. *See Fleites*, 617 F. Supp. 3d at 1157.
42. *Osborne v. Ohio*, 495 U.S. 103, 111 (1990).
43. *MG Freesites, Ltd.*, 2022 WL 407147, at \*22.
44. *Id.*
45. *Paroline v. United States*, 572 U.S. 434, 457 (2014).
46. *Id.*; *see also United States v. Garcia*, No. 19CR4488-JLS (S.D. Cal. Dec. 14, 2021), <https://casetext.com/case/united-states-v-garcia-2562> (ordering operators of GirlsDoPorn website to pay restitution to victims after being sentenced for criminal conspiracy to commit sex trafficking).
47. *Prewett v. Weems*, 749 F.3d 454, 457 (6th Cir. 2014).
48. *Smith v. Husband*, 376 F. Supp. 2d 603, 607 (E.D. Va. 2005).
49. 18 U.S.C. §2255 (2022).
50. *Doe v. Boland*, 698 F.3d 877, 880 (6th Cir. 2012).
51. *Lemmon v. Snap, Inc.*, 995 F.3d 1085, 1094 (9th Cir. 2021).
52. *A.M. v. Omegle.com, LLC*, 614 F. Supp. 3d 814, 821 (D. Or. 2022).
53. *Gonzalez v. Google LLC*, 2 F.4th 871, 912–13 (9th Cir. 2021), *reversed on other grounds*, 598 U.S. 617 (2023).
54. *Doe v. Internet Brands, Inc.*, 824 F.3d 846, 854 (9th Cir. 2016).
55. *Gonzalez*, 598 U.S. at 622.
56. *In Re: Social Media Adolescent Addiction/ Personal Injury Prods. Liab. Litig.* (MDL No. 3047) (N.D. Cal.); *Social Media Cases* (JCCP No. 5255) (Cal. Super. Ct.).
57. Order at 57-66, 86-87, *Social Media Cases* (JCCP No. 5255) (Cal. Super. Ct.) (Oct. 13, 2023).
58. For example, Bark, Net Nanny, Qustodio, and Canopy.