WHO’S ACCOUNTABLE: SHOULD A GLOBAL ISSUE CHANGE AMERICA’S INTERNET LAWS?

Jennifer P. Santos*

I. INTRODUCTION

Child pornography could not exist at the magnitude it does today without the development and advances of technology in the last twenty years.1 While it is evident to most of society that child pornography is a problem to be addressed, there is debate on what implementations are necessary to regulate the flow of child pornography on the Internet.2 Congress has passed Internet regulation laws in an attempt to stop the production and distribution of child pornography.3 Nevertheless, the rapid evolution of technology has left

---

* J.D. Candidate, Suffolk University Law School, 2023.
1 See Devon Ishii Peterson, Child Pornography on the Internet: The Effect of Section 230 of the Communications Decency Act of 1996 on Tort Recovery for Victims Against Internet Service Providers, 24 Hawai’i L. Rev. 763, 764 (2002) (illustrating how “[t]he Internet is one of the most exciting and powerful technological developments of the twentieth century.”). This comment further states, “[c]hild pornography simply could not exist anywhere near its current magnitude without recent technological advances.” Id. at 766. “While the Internet appears to have almost unlimited potential for improving lives, it is also helping to further criminal activity.” Id. at 764.
2 See Lesli C. Esposito, Regulating the Internet: The New Battle Against Child Pornography, 30 Case W. Res. J. Int’l L. 541, 562–63 (1998) (comparing how other nations have attempted to regulate the transmission of child pornography on the Internet). Regulations should start at a national level, however, there must be an international structure to monitor national efforts in order to ensure the success of those efforts. Id.
3 See Mitchell P. Goldstein, Congress and the Courts battle over the First Amendment: Can the Law Really Protect Children from Pornography on the
law makers out of breath as they try to keep pace with the continuous technological evolutions.4

Internet Service Providers (“ISPs”), including social media sites, search engines, and big tech companies have developed with little legislative framework.5 Without effective legal safeguards, these ISPs could be escaping liability with no justice for the victim.6 Many speculate there is no perfect balance between holding ISPs responsible for content on their websites and restricting speech online, causing First Amendment rights to be at stake.7

Increasing liability for online service providers that contribute to the spread of child pornography may create a larger incentive to monitor their services. There have been attempts made by big tech companies to help law enforcement in controlling the distribution of child pornography and some of these efforts have been scrutinized for evasion of privacy. Increasing liability could mean reducing certain privacies online, but the benefits might outweigh the harms when it comes to preventing the spread of child pornography. Requiring platforms to provide users with mechanisms to flag unlawful child pornography may be the balance needed to protect privacy rights while also clearing the Internet of child pornography.

4 See William P. Barr, Att’y Gen., Opening Remarks at the DOJ Workshop on Section 230: Nurturing Innovation or Fostering Unaccountability? (Feb. 19, 2020) (recognizing due to the nature of the Internet today and the reliance Americans have on the Internet there is a need to consider reforming laws around regulating the Internet). See also U.S. DEP’T OF JUST., SECTION 230 — NURTURING INNOVATION OR FOSTERING UNACCOUNTABILITY? (2020) at 1 [hereinafter KEY TAKEAWAYS AND RECOMMENDATIONS] (analyzing online platforms immunity from “a wide array of illicit activity on their services and free to moderate content with little transparency or accountability.”).

5 See Murdoch Watney, The Evolution of Internet Legal Regulation in Addressing Crime and Terrorism, 2 J. DIGIT. FORENSICS, SEC. & L. 41, 43 (2007) (overviewing the evolution of legal regulations on the Internet). “The Internet was not founded on a secure foundation” rather it was meant to be open, and this led to the increase of online crimes. Id.

6 See id. (illustrating how cybercrimes were different than crimes committed in the past). There became a need to change from a self-regulating system of legal regulation in order to criminalize conduct on the Internet. Id. at 43–44.

II. HISTORY

A. First Amendment Does Not Apply to Child Pornography

The revolutionization of technology and advancement of the Internet lies parallel to the explosion of child pornography. Before the Internet became widely convenient and confidential in the late 1970s, pornography was sold in stores. During this time, America became aware of the problem of child pornography and moved to make the production, distribution, and even possession of child pornography illegal. As a result of increased public attention on the problem of child pornography being shared today. Most Americans are unaware that “70 million online images and videos of child pornography were reported to law enforcement in 2019 alone[.]”

8 See Peterson, supra note 1, at 764–65 (illustrating how the Internet has changed the way child pornography is produced and distributed). Further stating, “[w]hile the Internet appears to have almost unlimited potential for improving lives, it is also helping to further criminal activity.” Id. at 764. See also Erin Freilich, Americans Are Acutely Unaware of the Prevalence of Child Sex Exploitation Online, New Study Finds, N.Y. SOC’Y FOR PREVENTION CRUELTY TO CHILD. (Dec. 10, 2020), archived at https://perma.cc/2NMQ-W6DR (describing the prevalence of child pornography being shared today). Most Americans are unaware that “70 million online images and videos of child pornography were reported to law enforcement in 2019 alone[.]”

9 See Howard A. Davidson & Gregory A. Loken, Nat’l Legal Res. Ctr. for Child Advoc. & Prot., No. 109927, Child Pornography & Prostitution Background & Legal Analysis 1 (1987) [hereinafter CTR. FOR CHILD ADVOC. & PROT.] (discussing the availability of child porn in the 1970’s). Further, in 1977 there were at least 260 different monthly publications of child porn in the United States. Id. See generally City of L.A. v. Alameda Books, 535 U.S. 425, 435–38 (2002) (raising the issue of whether a city could ban adult stores after a study found that crime rates were higher in places where there is an increased number of adult stores). See also Cassell Bryan-Low, Child porn is lucrative criminal trade on Internet, WALL ST. J. (Jan. 17, 2006), archived at https://perma.cc/FZR3-K73W (explaining in the 1980s the U.S. and other countries had largely restricted the flow of child pornography by prohibited it from being sold in stores). But the Internet changed the flow as Kevin Zuccato, director of the Australian federal police’s high-tech crime center explained that, “people who had never dreamed of indulging in the fantasy” were able to access child pornography online. Id.

10 See CTR. FOR CHILD ADVOC. & PROT., supra note 9, at 1 (explaining the late 1970s is when child porn “had become a highly organized industry that operated on a nationwide scale.”). The report estimates that child porn grossed a half-billion to a billion dollars a year. Id. Further, in the 80’s there was a shift in the materials being sold individually through private communications. Id. at 2. See also Elaine Shannon, Main Street Monsters, TIME (Sept. 14, 1998), archived at https://perma.cc/C4TC-FSCZ (describing the dangers of a secret international ring
child pornography, the New York Supreme Court ruled child pornography is not protected by the First Amendment, even if it was not obscene.11 In New York v. Ferber, the adult bookstore owner, Paul Ferber, was caught selling child pornography and argued his First Amendment rights to freedom of speech protected him in doing so.12 The court upheld the constitutionality of punishing Ferber for selling child pornography because the government has a compelling interest in preventing the sexual exploitation of children.13

B. Internet Advancements Calls for Congressional Actions

The crackdown on the production and distribution of child pornography was a victory and remained so until the Internet dramatically altered the landscape.14 Throughout the 1970s and 1980s Congress passed legislation to address the technological developments in regards to child pornography and eventually criminalized

of child pornographers). Law enforcement officials found 500,000 images of children and stated that membership to these secret child porn sharing clubs was limited to individuals who could prove they owned thousands of images of child pornography. Id.

11 See New York v. Ferber, 458 U.S. 747, 761 (1982) (finding that child pornography may be banned without first being deemed obscene because the government has a compelling interest in preventing the sexual exploitation of children). See also Miller v. California, 413 U.S. 15, 36–37 (1973) (ruling that the First Amendment allowed for the regulation of obscene material).

12 See Ferber, 458 U.S. at 751–52 (detailing how Paul Ferber, an owner of an adult bookstore in Manhattan, sold an undercover police officer two films depicting young boys masturbating and subsequently was charged with promoting both obscene sexual performances and indecent sexual performances).

13 See Artemus Ward, Child Pornography, FIRST AMEND. ENCYC. (Jan. 28, 2022), archived at https://perma.cc/K7W8-F8RS (explaining “[t]he overriding concern of legislators in criminalizing child pornography is its link to the actual sexual abuse of children, a justification generally sustained by courts despite First Amendment free speech objections.”). See also Osborne v. Ohio, 495 U.S. 103, 110–11 (1990) (extending the logic of Ferber to private possession of child pornography).

transporting, distributing, or receiving child pornography via computer. But a study later published in 1995, by Marty Rimm at Georgetown University’s Law Review, declared that 83.5% of images on “Usenet” were pornographic in nature. The finding of the study was published in *Time Magazine* spreading concern across America about the unwanted prevalence of pornography, especially for children as viewers. Senator James Exon proposed legislative regulations in an effort to protect America’s children by offering a measure never done before: regulate speech on the Internet. Exon’s main goals were to make the transmission of obscene and indecent material illegal.

---

15 See U.S. Sent’g Comm’n, The History of the Child Pornography Guidelines 8–9 (2009) (discussing the congressional concern that originally came to light in the late 70s and the steps made by Congress to set punishment standards for the production and distribution of child pornography).

16 See Robert Cannon, The Legislative History of Senator Exon’s Communications Decency Act: Regulating Barbarians on the Information Superhighway, 49 Fed. Commc’ns L.J. 51, 53 (1996) (citing Marty Rimm, Marketing Pornography on the Information Superhighway: A Survey of 917,410 Images, Descriptions, Short Stories, and Animations Downloaded 8.5 Million Times by Consumers in Over 2000 Cities in Forty Countries, Provinces, and Territories, 83 Geo. L.J. 1849, 1867, 1914 (1995) [hereinafter Rimm Study]) (discussing the evolution of child pornography on the Internet). This study was eventually found to be inaccurate. Id. at 55–57. See also USENET, BRITANNICA (Feb. 28, 2022), archived at https://perma.cc/V2JZ-SZXN (explaining that Usenet is an early system that allowed for worldwide discussion via a network of servers with computers around the world). Usenet was an early precursor to the Internet. Id.

17 See Cannon, supra note 16, at 54 (commenting on Time’s publication of the Rimm Study). The problem with pornography was how available it had become because of the Internet. Id. at 53.

18 See Cannon, supra note 16, at 52–57 (discussing Senator Exon’s reasoning for advocating for the passage of the CDA). Senator Exon believed he was “introducing the most important piece of legislation” because it provided much needed protection for children against pornographers. Id. at 57. Interestingly, Senator Exon had no firsthand experience with the Internet, he always had a staff member download what he wanted. Id. at 72. “Senator Exon’s Washington, D.C., offices had no e-mail address and had no office hook-up to the Internet.” Id. See also Mary Grav Leary, The Indecency and Injustice of Section 230 of the Communications Decency Act, 41 Harv. J. L. & Pub. Pol’y 553, 559 (2018) (describing the CDA was a way to prohibit the known “dissemination of obscene material to children[,]”). The CDA also sought to incentivize tech companies to block explicit material from reaching children. Id.

19 See Cannon, supra note 16, at 77–78 (defining obscenity and indecency). See generally Miller v. California, 413 U.S. 15, 24 (1973) (delineating the current three-pronged test for obscenity). See also Memoirs v. Massachusetts, 383 U.S. 413, 419 (1966) (stressing that under the Roth obscenity test, a work must be utterly without
This measure was met with opposition as adversaries, mostly tech companies, feared overregulation in an industry that was just beginning to expand. The fears were warranted as shortly after Exon’s proposal, the New York Superior Court, in Stratton-Oakmont v. Prodigy Servs. Co., held a tech company liable as “publishers” for content on its website when the company regularly monitor what users posted. The Stratton-Oakmont ruling put companies in a catch-22, where they had to either advantageously limit illegal activity or not monitor their websites and shield themselves from liability.

C. Adoption of Section 230 of the Communication Decency Act

Only five weeks after the Stratton-Oakmont decision, Congress created Section 230 of the Communications Decency Act of 1996 (“CDA”) to remove website owners’ liability of any illegal activity posted by third parties. With the adoption and interpretation of the social value before it can be considered obscene). See also Roth v. United States, 354 U.S. 476, 485 (1957) (holding that “obscenity” is not protected speech). Under this approach the Court is developing a definition of speech that can be banned. Id. See Lorraine Mercier, The Communications Decency Act, Congress’ First Attempt to Censor Speech over the Internet, 9 LOY. CONSUMER L. REV. 274, 284–86 (1997) (calling attention to the constitutional challenges of the CDA). See also Reno v. ACLU, 521 U.S. 844, 849 (1997) (finding the CDA violates the individuals constitutionally protected right to free speech). The anti-indecency provision of the CDA violated freedom of speech. Id. at 883. The Supreme Court struck down as vague some of the more controversial criminal provisions of the CDA, such as the prohibition of the transmission of “indecent material.” Id. at 871–72. See also Leary, supra note 18, at 559 (stating “[b]ecause the CDA regulates the Internet, many tech companies opposed it in principal and fought it at every opportunity.”). Opponents of the CDA were concerned that “service providers would be held criminally liable for providing minors with access to the Internet.” Id. at 560. See Stratton Oakmont v. Prodigy Servs. Co., No. 31063/94, 1995 N.Y. Misc. LEXIS 229, at *17–18 (holding Prodigy liable as publishers when allowing users to post criminal and fraudulent material against the plaintiff’s company). The court reasoned that because it voluntarily deleted some messages it was therefore legally responsible for the defamatory messages it failed to delete. Id. See Carlin Meyer, Reclaiming Sex from the Pornographers: Cybersexual Possibilities, 83 GEO. L.J. 1969, 1983 (1995) (commenting on impossibility of monitoring all transmissions over server computers).

21 See Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997) (finding that “Congress enacted § 230 to remove the disincentives to self-regulation created by the Stratton Oakmont decision.”). The court reasoned that “[i]t would be impossible for service providers to screen each of their millions of postings for possible problems.” Id. at 327. The tort liability created by holding service providers liable for their users posting would “have an obvious chilling effect.” Id. See also Leary, supra note 18, at 560 (Congress was prompted by the concerns of tech companies to add Section 230 to the CDA). “[T]he origin and entrenchment [of Section 230]
CDA Congress led the country down a perilous path as ISPs were no longer accountable for what their users posted including child pornography. The CDA amended the telecommunications law by making it illegal to knowingly send to, or show, minors obscene or indecent content online. The CDA was created for two purposes: (1) promoting the innovation of the Internet, and (2) helping ISPs moderate their content without fear of legal liability for illegal content shared by their users. Despite the vague language of the CDA, reveal a great deal about the values of the technology industry and the U.S. Congress.” Id. at 554. Section 230 may be part responsible for the growth of the Internet because it provided protections for websites. Id. “It is clear that, whatever § 230 did for the legitimate digital economy, it also did for the illicit digital economy.” Id. 24 See Commcn Decency Act of 1996, 47 U.S.C. § 230 (1996) (passing the Act was Congress’s attempt to make the Internet safer for children and ensure the development of the Internet). See also Derek E. Bambauer, Trump’s Section 230 reform is repudiation in disguise, BROOKINGS (Oct. 8, 2020), archived at https://perma.cc/D4DR-TFUA (stating, “[i]n thanks to Section 230, [ISPs] they mostly can’t be sued for the content their users create”). “Section 230 grants internet platforms legal immunity for most of the content posted by their users and provides the legal basis for platforms like Facebook and Twitter to operate without fears of ruinous liability.” Id. See generally Dart v. Craigslist, Inc., 665 F. Supp. 2d 961, 969 (N.D. Ill. 2009) (holding § 230 of the CDA protected a website from claims that the website facilitated prostitution). Dart, Sheriff of Cook County, sought to take down Craigslist which was the largest source of prostitution in the country, but the court ruled Craigslist was immune from wrongs committed by their users under Section 230. Id. at 968. See also Barr, supra note 4, at 2 (describing the statute as a way to nurture emerging Internet businesses while also incentivizing them to regulate harmful online content). Courts have interpreted Section 230 immunity so broadly that it has been diverging from its original purpose. Id. See also Child Pornography Prevention Act of 1996, 18 U.S.C.S. § 2252A (1996) (banning virtual child pornography). But see Ashcroft v. Free Speech Coal., 535 U.S. 234, 257–58 (2002) (striking down portions of the federal Child Pornography Prevention Act that banned “virtual child pornography,” which the justices said was neither obscene nor actual child pornography as defined by previous decisions). The material in question was made using computer imaging and banning adults who appeared to be minors was a violation of the fight to freedom of speech. Id. at 256. 25 See Cannon, supra note 16, at 92 (describing the “most comprehensive reform of telecommunications law since 1934”). The amendment was highly debated, some felt the Internet would harm society if it was uncontrolled, making it necessary for the government to protect the people. Id. at 93. Others felt the Internet was an opportunity “unlike anything before” and would improve the quality of society. Id. 26 See Sona Movsisyan, Human Trafficking in a Digital Age: Who Should Be Held Accountable?, 27 MICH. ST. INT’L L. REV. 539, 554 (2019) (discussing the purpose of Section 230 is for development of free speech and allow online service to implement their own standards). The CDA has unforeseen implications due to the blanket
protecting the growth of the internet and free speech were enough to let it pass.\textsuperscript{27} Seeing the Internet as largely beneficial to society, the CDA intended to create Section 230 to promote Internet growth by ensuring to reduce the threat of litigation for ISPs.\textsuperscript{28} Section 230 immunity in both civil and criminal litigation. \textit{Id. See also} Katy Noeth, \textit{The Never-Ending Limits of §230: Extending ISP Immunity to the Sexual Exploitation of Children}, 61 \textit{Fed. Comm. L.J.} 756, 768 (2008) (discussing legislative intent behind enacting § 230 in 1996). Section 230 of the CDA and the legal protection it provides to ISPs is unique to the United States. \textit{Id. See also} Leary, \textit{supra} note 18 (discussing the purpose of Section 230 was a “component of a broader effort to limit access to explicit material through the Internet.”).

\textsuperscript{27} \textit{See} Barr, \textit{supra} note 4, at 2 (announcing the Department of Justice’s concern about the expansively broad interpretation of Section 230).

The courts’ broad interpretation of Section 230 also occurs against the background of the Supreme Court, in 1997, striking down every other provision of the CDA on First Amendment grounds. This left in place an unbalanced statutory regime that preserves technology providers’ liability protections, without guaranteeing corresponding protections for minors from harmful material on the Internet.

\textit{Id. See also} Noeth, \textit{supra} note 26, at 766–67 (Section 230 of the CDA bars claims against ISP’s based on the publication of third-party content).

Defendants are immune from liability from state law claims if: (1) [They are] a ‘provider or user of an interactive computer service’; (2) the claim is based on ‘information provided by another information content provider’; and (3) the claim would treat [the Defendants] ‘as publisher or speaker’ of that information.

\textit{Id. See} Noeth, \textit{supra} note 26, at 768 (discussing legislative intent behind enacting § 230 in 1996). \textit{See} Leary, \textit{supra} note 18, at 559 (discussing the purpose of Section 230 was a “component of a broader effort to limit access to explicit material through the Internet.”). \textit{See} Elizabeth Nix, \textit{The World’s First Web Site, HISTORY} (Aug. 30, 2018), \textit{archived at} https://perma.cc/VVA7-8LVN (explaining the history of the World Wide Web). Berners-Lee, creator of the Web was named one of time Magazine’s 100 Most Important People of the 20\textsuperscript{th} Century and is quoted saying “this is for everyone.” \textit{Id. See generally} Anmar Frangoul, \textit{10 ways the web and internet have transformed our lives}, \textit{CNBC} (Feb. 9, 2018), \textit{archived at} https://perma.cc/BA64-ZT9S (citing search engines, ecommerce and social media as some of the ways the Internet has drastically changed our lives); Caitlin Dewey, \textit{36 ways the Web has changed us}, \textit{WASH. POST} (Mar. 12, 2014), \textit{archived at} https://perma.cc/VT8G-MNWS (listing 36 ways the Web has changed our lives and the world in general). The “4 billion indexed Web pages” has impacted the world and also destroyed somethings along the way like a purpose for watches, phone books, and music stores. \textit{Id.}
reflects Congress’s desire to protect ISPs from liability for unlawful third-party content, like child pornography.  

**D. Escaping Accountability as Congress Expands Immunity**

Over the next decade, case law expanded the broad immunity created from Section 230. When America Online (“AOL”) was sued in 1997 for comments posted by a user, the Fourth Circuit concluded that Section 230 barred any cause of action that would make service providers responsible for information posted by a third-party user.  

---

29 See Noeth, supra note 26, at 766–67 (Section 230 of the CDA bars claims against ISP’s based on the publication of third-party content). Defendants are immune from liability from state law claims if: (1) [They are] a ‘provider or user of an interactive computer service’; (2) the claim is based on ‘information provided by another information content provider’; and (3) the claim would treat [the Defendants] ‘as publisher or speaker’ of that information.  

Id. See also Michael H. Keller & Gabriel J.X. Dance, The Internet is Overrun With Images of Child Sexual Abuse. What Went Wrong?, N.Y. TIMES (Sept. 29, 2019), archived at https://perma.cc/8DXP-CDPK (illustrating how reports of child pornography has exploded in recent years). Child pornography has been shared for decades “but it has never been like this: Technology companies reported a record 45 million online photos and videos of the abuse last year.” Id. “[M]any tech companies failed to adequately police sexual abuse imagery on their platforms, or failed to cooperate sufficiently with the authorities when they found it. Law enforcement agencies devoted to the problem were left understaffed and underfunded, even as they were asked to handle far larger caseloads.” Id.  

30 See Ben Ezra, Weinstein, & Co. v. Am. Online, Inc., 206 F.3d 980, 986 (10th Cir. 2000) (holding that America Online could not be sued by Ezra for providing wrong information about him because third-party companies "alone created the stock information at issue."). AOL could not be held liable for defamation when it displayed the stock quotes on its site. Id. See also Blumenthal v. Drudge, 992 F. Supp. 44, 50 (D.D.C. 1998) (finding the Drudge Report immune from liability for story that plaintiff abused his wife). But see Doe v. Am. Online, Inc., 783 So.2d 1010, 1012–13 (Fla. 2001) (granting AOL immunity from a negligence claim of marketing child pornography).  

31 See Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) (basing the decision on a desire to incentivize companies to self-regulate). The court reasoned that ruling the opposite way would expose service providers to liability if they knew of defamatory messages on their space, and that this, in turn would incentivize them to be willfully ignorant and to cease policing their websites. Id. Immunity provision under § 230(c) states that the lawsuits seeking to hold a service provider liable for its exercise of a publisher’s traditional editorial functions are barred. Id. See also David
Similarly in *Doe v. Bates*, *Doe v. MySpace, Inc.*, and *Doe v. SexSearch.com*, the courts extended Section 230’s immunity by refusing to hold ISPs liable for failing to police their sites for harmful content posted by users. The court found that requiring ISPs to screen for potentially obscene material, or to even respond to notices, would not be feasible because the sheer number of postings would create an impossible burden. The courts in these cases have shown a willingness to extend Section 230 immunity from defamations suits to child exploitation claims, even when it enables sexual predators to prey on minors.

### E. Fighting Child Pornography

Since the creation of the highly controversial Section 230 of the CDA, Congress has passed several acts to combat the issues...
created by broad immunity for ISPs. The Protect Our Children Act of 2008, sponsored by President Joe Biden, created the reporting requirement for tech companies to detect child pornography on their sites. The Senate passed Allow States and Victims to Fight Online Sex Trafficking Act (“FOSTA”) in 2018, which created an exception to Section 230 of the CDA. The need for reform became apparent in 2020 when Attorney General William Barr and the Department of Justice (“DOJ”) held a workshop dedicated to brainstorming ideas for Section 230 reform. Attorney Barr expressed concern for the unbalanced Section 230 because it protected tech companies from liability without protecting children from harmful material online. With the recent movement of Congress, Section 230’s contradictory

37 See also Seynep Ulku Kahveci, Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA): Senate Passes Bill Making Online Platforms Liable for Third-Party Content Enabling Illegal Sex-Trafficking, JOLT DIG. (Apr. 4, 2018), archived at https://perma.cc/5C7R-D49V (describing the history of the Act and how it came to be). “The bill includes an affirmative defense for those who live in states where prostitution is legal.” Id. “A coalition of Internet companies — including Reddit, Twitter, GitHub, The Wikimedia Foundation, and Yelp — have signed a letter protesting the legislation.” Id.
38 See Barr, supra note 4, at 1 (announcing the Department of Justice’s efforts to keep up with rapidly changing technology). See also Biden v. Knight First Amendment Inst. at Columbia Univ., 141 S.Ct. 1220, 1226 (2021) (Thomas, J., concurring) (suggesting that Section 230 is outdated and that tech platforms might instead be regulable as "common carriers").
39 See Barr, supra note 4, at 2 (discussing the Department of Justice’s concern about the expansively broad interpretation of Section 230).

The courts’ broad interpretation of Section 230 also occurs against the background of the Supreme Court, in 1997, striking down every other provision of the CDA on First Amendment grounds. This left in place an unbalanced statutory regime that preserves technology providers’ liability protections, without guaranteeing corresponding protections for minors from harmful material on the Internet.

Id.
purpose in attempting to keep children safe has actually made them vulnerable to the industry of child pornography.\textsuperscript{40}

Recognizing the growing problem, Congress proposed clarifying Section 230 of the CDA by creating the Fight Online Sex Trafficking Act (“FOSTA”) to hold websites liable for consistently using their sites as marketplaces for human trafficking.\textsuperscript{41} After years of ISPs and online marketplace sites using Section 230 as a shield, politicians wanted a way to hold these sites liable.\textsuperscript{42} The website Backpage, a site similar to Craigslist, was charged with pimping a minor and trafficking in 2016 after continuously publishing advertisements for sex acts, but they escaped liability for years based on Section 230 immunity.\textsuperscript{43} FOSTA provided clarity that victims are not limited from using their private right of action against the websites that sell them.\textsuperscript{44}

\textsuperscript{40} See Peterson, supra note 1, at 764–65 (finding “[t]he CDA, designed to protect children on the Internet, actually absolves Internet service providers (“ISPs”) of responsibility for the criminal distribution of child pornography on websites.”).

\textsuperscript{41} See Caitlyn Burnitis, Facing the Future with FOSTA: Examining the Allow States and Victims to Fight Online Sex Trafficking Act of 2017, 10 U. MIA. RACE & SOC. JUST. L. REV. 139, 147 (discussing the development and passage of FOSTA). See also Gregory M. Dickinson, Rebooting Internet Immunity, 89 GEO. WASH. L. REV 347, 352 (stating that amending Section 230 to withhold immunity was stemmed from the growing problem of ISP profiting from unlawful content). “Internet immunity reform continues to face significant opposition, however, from the tech industry and from those legal scholars who worry that changes to Section 230 could do more harm than good.” Id. at 352–53.

\textsuperscript{42} See Wagner Trafficking Bill Headed to House Floor, CONGRESSWOMAN ANN WAGNER MO. 02 (Feb. 21, 2018), archived at https://perma.cc/7Y4F-EFE3 (announcing the passage of a bill that would clarify that Section 230 of the CDA does not prevent states and victims of sex trafficking from pursuing justice). The bill had the purpose of helping to provide the remedies to victims. Id. “[W]e are shutting down the loophole that allows websites like Backpage.com to facilitate the sale of our children for sex[.]” Id. See also Eric Goldman, Congress Probably Will Ruin Section 230 This Week (SESTA/FOSTA Updates), TECH. & MKTG. L. BLOG (Feb. 26, 2018), archived at https://perma.cc/8NMS-X3JB (arguing that the passing of SESTA/FOSTA would ruin the protections offered by Section 230).

\textsuperscript{43} See Christopher Mele, C.E.O. of Backpage.com, Known for Escort Ads, Is Charged with Pimping a Minor, N.Y. TIMES (Oct. 6, 2016), archived at https://perma.cc/T2EC-KGXD (explaining how the charges were filed in California Superior Court). The individuals arrested were not charged with trafficking minors. Id.

\textsuperscript{44} See Wagner Trafficking Bill Headed to House Floor, supra note 42 (articulating the purpose of FOSTA/SESTA). See generally Wendy Davis, Backpage Urges Supreme Court to Reject Appeal Over Escort Ads, MEDIAPOST (Dec. 1, 2016), archived at https://perma.cc/W9B8-6BY3 (explaining how Backpage is pleading to the United States Supreme Court to “let stand a decision dismissing a lawsuit against the company by a group of sex-trafficking victims.”).
With the creation of Section 230 of the CDA, Congress opened a floodgate for the Internet to become a means for advertising the availability of children for sex.\textsuperscript{45} Congress recognized that the CDA was never intended to help facilitate sex trafficking and thus created FOSTA to control illegal activity online.\textsuperscript{46} FOSTA formed an exception to the broad immunity, finding that the CDA does not protect against civil liability or criminal charges of facilitating human trafficking and prostitution online.\textsuperscript{47} Websites like Backpage, because of FOSTA, are now prevented from knowingly facilitating sex trafficking by using Section 230 as a shield.\textsuperscript{48}

To encourage tech companies to take preventative measures in monitoring their platforms for child pornography, the Senate Judiciary Committee introduced the first draft of the Eliminating Abusive and Rampant Technologies Act ("EARN IT Act") in March 2020.\textsuperscript{49}

\textsuperscript{45} See Backpage.com, LLC v. Cooper, 939 F. Supp. 2d 805, 823 (M.D. Tenn. 2013) (concluding that criminal statutes are inconsistent with § 230). “The Internet has become a favored means of advertising the availability of children for sex because advertisements can be purchased more rapidly than in other media, allowing pimps to move victims to different locations quickly.” Id. at 815. Further, the court treats Backpage as a publisher of third-party users, thus preempted by the CDA. Id. at 827–28.

\textsuperscript{46} See Burnitis, supra note 41, at 148–49 (explaining how FOSTA was signed into effect by President Trump in 2018 as primarily amending Section 203 of the CDA). “In passing FOSTA, Congress contended that Section 230 immunity was never intended to provide a broad umbrella of legal protections for websites that were knowingly and unlawfully promoting, advertising, or facilitating prostitution, or for websites that were facilitating the sale of sexual acts by those being sexually trafficked.” Id. at 142.

\textsuperscript{47} See Tom Jackman, Trump signs ‘FOSTA’ bill targeting online sex trafficking, enables states and victims to pursue websites, WASH. POST (Apr. 11, 2018), archived at https://perma.cc/QG2G-HXQM (headlining Trump signing the FOSTA bill). The signing was shortly after the seven executives from Backpage.com had been arrested and charged for using their website to facilitate prostitution. Id. The bill gave prosecutors the tools they needed to criminalize online markets for prostitution. Id. Critics of the bill argue this deprives sex workers from the ability to safely screen customers. Id.

\textsuperscript{48} See Burnitis, supra note 41, at 151 (elaborating the goal of FOSTA is to create an exception to the broad immunity that was created by Section 230 in order to prevent websites from knowingly facilitating sex trafficking). “At the heart of this law was the desire to ensure that websites like Backpage were unable to continue to knowingly facilitate sex trafficking by using Section 230 as a shield.” Id. at 150–51.

\textsuperscript{49} See Cat Zakrzewski, A bill aiming to protect children online reignites a battle over privacy and free speech, WASH. POST (Feb. 10, 2022), archived at https://perma.cc/YKQ3-87HE (discussing the purpose of the EARN IT Act). See also Graham, Blumenthal, Hawley, Feinstein Introduce EARN IT Act to Encourage Tech
introducing the EARN IT Act, the Senate Judiciary Committee intended to hold tech companies accountable for the creation and distribution of child pornography by recommending the best practices for identifying and reporting child pornography online.\textsuperscript{50} The first draft of the EARN IT Act required tech companies to “earn” Section 230 immunity by following the Act’s “best practices” and the Attorney General (“AG”) had the ultimate power in determining the best practices.\textsuperscript{51} After criticism, the Act has since been revised several times to develop the best practices that tech companies would have to adopt to get the protective immunity offered by Section 230.\textsuperscript{52}

Previously, the EARN IT Act would have left ISPs liable for a broad amount of civil penalties if they recklessly, rather than knowingly, distributed child pornography on their platforms.\textsuperscript{53} Amended versions of the Act removed the proposed reckless standard and kept a knowledge standard.\textsuperscript{54} Additionally, any Internet planform

\textit{Industry to Take Online Sexual Exploitation Seriously,} COMM. ON JUDICIARY (Mar. 5, 2020), archived at https://perma.cc/XZ4X-2KP9 (stating the EARN IT Act “would create incentives for companies to ‘earn’ liability protection for violations of laws related to online child abuse material (CSAM).”).\textsuperscript{50} See Emily Birnbaum, Am\textit{endments to the EARN IT Act could resolve its encryption issues,} PROTOCOL (July 1, 2020), archived at https://perma.cc/EBD2-T5EW (stating “the EARN IT Act, the most serious congressional threat to Section 230 since SESTA/FOSTA, would require online companies to seriously crack down on online child sexual abuse material.”). See also Timothy Karr, The EARN IT Act: A Very Bad Bill Gets its Day in Congress, FREE PRESS (Mar. 11, 2020), archived at https://perma.cc/779Y-MYPR (noting that the legislation would create a congressionally appointed commission to develop best practices for tech companies).\textsuperscript{51} See Alan Z. Rozenshtein, The Revised EARN IT Act Proposes a Better Proposal for Encryption Policy, LAWFARE (Mar. 10, 2020), archived at https://perma.cc/54WC-F7H6 (explaining that one of the first drafts of the act was circulated in January of 2020). See also Birnbaum, supra note 50 (explaining that in July a “manager’s amendment” to the Act was published).\textsuperscript{52} See Rozenshtein supra note 51 (explaining that the draft of the act formally introduced to the senate in March contained “major revisions”). See also Marc Dahan, How the Earn IT Act could affect privacy, free speech and encryption, COMPARITECH (Oct. 23, 2020), archived at https://perma.cc/7MPZ-GTRU (explaining how the EARN IT Act was introduced to the Senate and that in the first draft “internet companies needed to ‘earn’ the protections of Section 230.”).\textsuperscript{53} See Birnbaum, supra note 50 (expressing the flaws in the EARN IT Act because it would make it harder to get rid of child pornography without violating Fourth Amendment rights to privacy). “‘The EARN IT Act remains a deeply flawed proposal that would make it harder for IA member companies to rid the internet of [child sexual abuse material] and protect the most vulnerable online,’ said Mike Lemon, the senior director of federal government affairs with the Internet Association.” Id.\textsuperscript{54} See id. (noting that under the amendment the “reckless” standard is removed, and the standard becomes “knowingly”). See also MODEL PENAL CODE § 2.02 (2)(b)
that knows of child pornography being distributed is required to take action by removing it and can be prosecuted if found to be in violation of this requirement.\(^{55}\) In advancing the EARN IT Act, Senators in opposition have echoed concerns from human rights groups that have suggested the Act does not support a proper balance between fighting child pornography and protecting users rights to privacy and encryption.\(^{56}\) The suggested “best practices,” have left many wondering if they allow law enforcement unrestrained access to users private communications on social media platforms.\(^{57}\)

\(^{55}\) See Joe Mullin, Key Senators Have Voted For The Anti-Encryption EARN IT Act, ELEC. FRONTIER FOUND. (Feb. 10, 2022), archived at, https://perma.cc/5M47-DBQL (highlighting how lowering the standard in which the state is allowed to prosecute ISPs for violating the requirement to remove child pornography is going to put more “pressure on [internet] companies to start doing widespread scanning of user messages and photos.”). See also Zakrzewski, supra note 49 (explaining how the EARN IT Act could harm encryption and security technologies that shield users’ privacy). “While law enforcement officials suggest the technology is a boon to criminals, including child predators, who can use it to evade detection, privacy advocates argue it’s a crucial protection for users online.” Id.

\(^{56}\) See Mullin, supra note 55 (advocating that the “harms will fall on the most vulnerable people” because the Act compromises encrypted data to be scanned for child pornography). “Once we allow encryption to be compromised to scan for CSAM, authoritarian regimes will demand the same capabilities to track information shared by activists and journalists. People subject to domestic abuse, including children, won’t have secure channels of communication to report and reach out for trusted help.” Id. See also Emily Anderson Stern, Bill intended to protect children online prompts outcry from privacy advocates, UNITED PRESS INT’L (Feb. 16, 2022), archived at https://perma.cc/4FLZ-MJ35 (explaining that under the EARN IT Act, social media companies will be expected to take responsibility of the content on their platforms). “Critics of the measure say this provision would disincentivize platforms from using encryption to protect users and would lead to unnecessarily censoring content in many cases.” Id.

\(^{57}\) See Mullin supra note 55 (articulating “[w]e all have a right to privacy, and to use encrypted services to protect our privacy.”).
III. FACTS

A. An International Problem

Images and videos of child pornography became more readily available through virtually every tech platform, including social networking sites, file-sharing sites, gaming devices, and mobile apps. The anonymous nature of the Internet is one of the reasons child pornography has become increasingly hard to detect, subsequently amplifying the prevalence of child pornography. Researchers have found the distribution of child pornography to be a very lucrative

58 See Keller & Dance, supra note 29 (reporting how the anonymity that tech platforms provide embolden criminals to post sexually abusive material of criminals). In the past, people would never been able to shop on the Internet for such horrific material, but now you can securely search for child pornography on any device. Id. See also Steven Malby et al., United Nations Off. on Drugs & Crimes, Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children 18 (2015) (demonstrating how new technology has allowed for a “cheap and easily accessible means of producing and widely distributing child sexual abuse material through the Internet[.]”). Prior to the Internet, producers of child pornography had to purchase expensive filming and copying equipment and ship videotapes or CD-ROM copies for distribution. Id.

59 See Peterson, supra note 1, at 770 (highlighting the Internet’s effect on the distribution and production of child pornography). See Freilich, supra note 8 (describing how most Americans are unaware that “70 million online images and videos of child pornography were reported to law enforcement in 2019 alone[,]”). See also Lesli C. Esposito, Regulating the Internet: The New Battle Against Child Pornography, 30 CASE W. RES. J. INT’L L. 541, 541 (1998) (asserting that the Internet, as an international system, has become the best hunting ground for pedophilia). The Internet has made the production and distribution of child pornography easy and anonymous. Id. “Also, pedophiles can now easily access child pornography from other countries, because for particular purposes, national boundaries do not exist in cyberspace.” Id. See also Child Sexual Abuse Statistics, Nat’l Ctr. for Victims of Crime (Nov. 18, 2021), archived at https://perma.cc/HK6U-D2M3 (finding the prevalence of child porn is hard to determine because it is often not reported). See also The Scourge of Child Pornography, FBI News (Apr. 25, 2017), archived at https://perma.cc/B5X6-4ZMM (reporting the prevalence of child pornography and the FBI’s work in fighting to prevent the spread of child pornography in an effort to protect children). Law enforcement further noted that the type of people who engage in the production and distribution of child pornography come from “all walks of life and represent varied ages, races, occupations and education levels.” Id. The crime is typically carried out on the dark web in order to remain anonymous, intending to keep their actions a secret from their spouses, families, and friends. Id. See also Alexander Kalim, Addressing the Gap in International Instruments Governing Internet Child Pornography, 21 COMM.LAW CONSPECTUS 428, 435 (2013) (addressing the depth of the problem of child pornography online and the difficulties measuring it because there is no governing body in place to police the activity).
business with a generated annual profit around $3 billion to $20 billion.

The true amount of available child pornography is hard to comprehend, due to its anonymous nature, but the National Center for Missing & Exploited Children accounts reported its CyberTipline has received over eighty-two million reports of child pornography worldwide. These numbers have led many nations and governments across the world to recognize the international effort that is needed to stop the flow of child pornography online.

B. International Laws Addressing Child Pornography

The Internet allows for cheap, instant, and confidential international exchanges of information and images, making child pornography an issue for the world to address in unison. There is a global lack of consensus on how to prevent and reduce the sharing of

---

60 See MALBY ET AL., supra note 58, at 19 (reporting that advances in technology have left victims of child pornography vulnerable to the demand for new images). Other estimates suggest the market is valued at $250 million a year. Id. at 34. While estimates vary, there is an agreement that the commercial child pornography material sector is large and lucrative. Id. See also Bryan-Low, supra note 9 (describing child pornography as the most lucrative trade on the Internet). See Katy Barnato & Bianca Schlotterbeck, Organized crime: World’s most lucrative criminal activities, CNBC (Aug. 9, 2013), archived at https://perma.cc/TQ6H-YK6H (listing child pornography along with drug trafficking and smuggling immigrants as the world’s most lucrative activities).

61 See The Scourge of Child Pornography, supra note 59 (illustrating six news articles from around the country that articulate crimes of child pornography). See also Child Sexual Abuse Material (CSAM), NAT’L CTR. FOR MISSING & EXPLOITED CHILD. (Nov. 18, 2021), archived at https://perma.cc/JAJ3-N83C (giving an overview of what child sexual abuse material is, who the victims are, the prevalence of the material reported).

62 See Esposito, supra note 2, at 543 (concluding that because the source and destination of child pornography are no longer necessarily in the same county thus the regulation of the criminal material must be international). Collaboration between nations is necessary and needs to be “attacked aggressively by all countries in order to be abolished.” Id.

63 See INT’L CTR. FOR MISSING & EXPLOITED CHILD., CHILD SEXUAL ABUSE MATERIAL: MODEL LEGIS. & GLOB. REV. 1, 1 (9th ed. 2018) [hereinafter MODEL LEGIS. & GLOB. REV.] (detailing the issues of children being vulnerable to those who seek child pornography because of the rapid growth of the Internet). “Children, every day, all around the world suffer sexual abuse and sexual exploitation at the hands of individuals who seek them out in order to fulfill their own sexual needs or to profit from the child’s exploitation.” Id.
child pornography due to variances in international laws. The United Nations Convention on Rights of the Child ("CRC"), has several international instruments to protect children from exploitation and many countries criminalize the production of child pornography, but countries differ on the concrete elements of the crime and the definitions of child. For example, some countries determine a person is a child based on age of consent, which can range from as low as thirteen to as high as twenty-one years old. The U.S. and the Convention on the Rights of the Child, identifies a child as anyone under the age of eighteen and some countries find age is irrelevant in gauging adulthood. Countries also vary in their consideration of virtual or simulated child pornography. Some countries criminalize simulated child pornography to a lesser extent, while countries like the United States and Sweden do not criminalize simulated child pornography due to variances in international laws.

64 See Malby et al., supra note 58, at 36 (acknowledging the increase in international laws recognizing children as deserving special protection, however, there is a variance between the degree to which international measures have been incorporated into national laws).

65 See id. (explaining the minimum standards of protection for children under the CRC). “The convention requires States Parties to take all appropriate measures at the national, bilateral or multilateral levels to prevent the inducement or coercion of a child to engage in any unlawful sexual activity[.]” Id. The CRC requires the adoption and implementation of legislation to criminalize and adequately punish child pornography and other child sexual abuse and exploitation material. Id. at 37. “While many [countries] criminalize acts such as production of [child pornography], they may differ on the concrete elements of the crime and the definitions of ‘child.’” Id. at 39.

66 See Kalim, supra note 59, at 432 (explaining that countries differ on a standard measurement or definition of a child, “which makes producing a neutral standard to gauge Internet child pornography difficult.”). Some countries define a child by when they are legally able to consent to sex or the legal age to vote. Id. A few even determine a child based on the age to legally get married. Id. at 433.

67 See id. at 438 (describing the United Nations Convention on the Rights of the Child and how child pornography was not recognized during the formation of the Convention in 1989).

68 See also Malby et al., supra note 58, at 42 (defining simulated child sexual abuse material as materials which feature adults disguised to look like children and virtual child sexual abuse material as visual materials that appear to be child pornography but are actually the product of digital creation).
The ambiguity in international laws regarding child pornography leaves certain children unprotected. The United States began cracking down on child pornography in the 1970s, there became an increase in demand to obtain these materials from other nations. Today we can see efforts that have been made by many countries, like India in their creation of Protection of Children from Sexual Offenses Act, in attempt to combat child pornography. There are currently numerous international efforts to combat child pornography.

---

69 See Ashcroft v. Free Speech Coal., 535 U.S. 234, 244 (2002) (holding simulated virtual child pornography legal because the First Amendment provides that “Congress shall make no law… abridging the freedom of speech.”). The dissent argued that rapidly advancing technology would soon make it difficult to distinguish between pornography made with actual children and that made with simulated images, however, Congress had a compelling interest in prohibiting child pornography. Id. at 267. See generally Dr. Al-Alosi, Virtual child pornography could both help and hinder law enforcement, THE CONVERSATION (Sept. 4, 2017), archived at https://perma.cc/38EE-YT25 (arguing now that virtual children look more realistic, it makes it harder to tell the difference between what is real and what is not). See also MALBY ET AL., supra note 58, at 42 (detailing that countries differ in their approach to criminalizing simulated child pornography). Only about one-third of countries include simulated material in their national laws on child pornography. Id. But see Prosecutor Remedies and Other Tools to End Exploitation of Children Today Act of 2003, Pub. L. No. 108–21, § 502, 117 Stat. 650 (2003) (prohibiting any digital or computer-generated image that is indistinguishable from that of a minor engaging in sexually explicit conduct).

70 See MODEL LEGIS. & GLOB. REV., supra note 63, at 36–60 (discussing the significant legislation over the last decade as more countries have developed laws to protect children). See generally Kristen Grienshaber, Germany busts international child porn site used by 400,000, ABC NEWS (May 3, 2021), archived at https://perma.cc/Y4R4-5GHV (reporting they have found four suspects in Paraguay, Hamburg, Munich, and Paderborn facilitating illegal child pornography online). More than 400,000 users were registered which German prosecutors announced to be “one of the world’s biggest international darknet platforms for child pornography[].”). Id.

71 See Esposito, supra note 2, at 552 (stating “Interpol, the international police agency, states that over 30,000 pedophiles are involved in organized child pornography rings in Europe, which began forming through the Internet.”). Europe became concerned as arrests were made in relation to an international child pornography ring. Id. at 552–53. Further stating, “[b]ecause pedophilia rings . . . have such strong ties to the Internet, many countries have launched efforts to halt the distribution of child pornography on the Internet.” Id. at 553.

72 See Milind Rajratnam, Combating Child Pornography in India, JURIST (May 14, 2020), archived at https://perma.cc/XA6J-3X35 (discussing India’s effort to combat child pornography by adopting the “Protection of Children from Sexual Offenses
conventions including the Council of Europe’s *Convention on Cybercrime* (Budapest Convention) that bolster countries respective laws to prosecute those involved in the production and distribution of child pornography.\textsuperscript{73}

As the gatekeepers to the Internet, ISPs are facing increasing pressure to implement reporting requirements and mechanisms to help regulate Internet content.\textsuperscript{74} In the United States and Australia, for instance, ISPs are required to report and identify child pornography published on their websites although they are not required to proactively search for the illegal material.\textsuperscript{75} Similarly in Canada, it is

\begin{itemize}
\item \textsuperscript{73}See \textit{Kalim supra} note 59, at 437 (compiling a list of the current international laws in place to address child pornography). Many international laws and treaties were created to establish an “effective action to prevent and combat trafficking in persons, especially women and children, . . . [in order] to punish the traffickers and to protect the victims of such trafficking[.]” \textit{Id.} at 440 n.82. \textit{See also} Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, May 25, 2000, 2171 U.N.T.S. 227 (creating the Optional Protocol on Sale of Children and Child Pornography in 2000 by the United Nations with the purpose to combat child pornography). \textit{See also} Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, Nov. 15, 2000, 2237 U.N.T.S. 319 (establishing an instrument to prevent and combat trafficking in persons, especially women and children). \textit{See also} \textit{Rajratnam, supra} note 72 (describing the Budapest Convention as the “foremost conventions that deal with child abuse as it has a more pragmatic approach with a universal application to both the judicial officers and the law enforcement agencies at the same time.”).
\item \textsuperscript{74}See \textit{Malby et al., supra} note 58, at 50 (discussing ISP’s opportunities to regulate and implement self-regulating strategies). \textit{See also} Frank Bajak & Barbara Ortutay, \textit{Apple to scan U.S. iPhones for images of child sexual abuse}, \textit{Associated Press} (Aug. 6, 2021), \textit{archived at} https://perma.cc/9YCJ-KG6Y (describing how “Apple has been under government pressure for years to allow for increased surveillance of encrypted data.”). \textit{See generally} Nicholas Kristof, \textit{The Children of Pornhub}, \textit{N.Y. Times} (Dec. 4, 2020), \textit{archived at} https://perma.cc/8CZJ-2T22 (giving accounts of child pornography victims and arguing that search engines, banks and credit card companies should be proactive in in impeding sites that share child pornography, like Pornhub).
mandatory for ISPs to report of child pornography and violators face fines or possible imprisonment.76 In extreme measures, the Chinese government has taken control by regulating ISPs and censoring everything including child pornography on the Internet.77 China has some of the strictest approaches on Internet regulations by requiring all Internet users to register with the authorities.78 Vietnam and Saudi Arabia have adopted similar approaches, by controlling access through a single Internet network controlled by the government.79

7, 2018), archived at https://perma.cc/98E9-WN22 (outlining that ISPs are required by 18 USC §2258A to report to the National Center for Missing or Exploited Children when they have knowledge of child pornography). ISPs are not required to actively search their sites or systems for illegal material. Id. But see Abigail Kuzma, A Letter to Congress: The Communications Decency Act Promotes Human Trafficking, 34 CHILD. LEGAL RTS. J. 23, 42 (explaining how even if there is a requirement to report illegal content, ISPs like Backpage does not remove the content). Every month Backpage reported 400 ads to the National Center for Missing and Exploited Children but in many instances the ads are not removed. Id.

76 See Yosie Saint-Cyr, Mandatory Reporting of Internet Child Pornography by Persons Who Provide an Internet Service Now Law, SLAW (Dec. 22, 2011), archived at https://perma.cc/H5SK-5E53 (detailing Canada’s federal act aimed at protecting children from online exploitation by requiring ISPs to report websites and notify the police by providing evidence of child pornography). See also ISP owners could face jail under child porn bill, CBC NEWS (Nov. 24, 2009), archived at https://perma.cc/CDF7-SR57 (clarifying that if enacted, ISPs would be required to report child pornography or face fines up to $100,000 and possible imprisonment if found to be the sole proprietor).

77 See Rebecca Davis, China’s New Internet Censorship Rules Outline Direction for Content, VARIOITY (Jan. 3, 2020), archived at https://perma.cc/A9LF-PXXA (reporting China’s new Internet regulations expand the online censorship in an attempt to block all negative content and make platforms more liable for content violations). See also Yvonne Lau, Here’s what Beijing’s sweeping new data rules will mean for companies, FORTUNE (Sept. 1, 2021), archived at https://perma.cc/ZAB4-F7H5 (reporting what China’s Internet censorship means for tech companies). Whether domestic or foreign companies that mishandle data will be punished harsher including heavy fines of criminal liability. Id.

78 See Davis, supra note 77(declaring China is “one of the world’s most censorious nations”). See also Freedom on the Net 2021 China, FREEDOM HOUSE (Nov. 21, 2021), archived at https://perma.cc/V2EZ-7W7Q (condemning China’s Internet censorship as oppressive and “the world’s worst abuser of internet freedom for the seventh consecutive year.”). This censorship is one of the most sophisticated in the world leaving Chinese users with access only to highly censored and monitored version of the Internet. Id.

79 See Justin Sherman, Vietnam’s Internet Control: Following in China’s Footsteps?, THE DIPLOMAT (Dec. 11, 2019), archived at https://perma.cc/939T-NY8V (assessing Vietnam’s measures to increase control over the Internet as the government monitors information and communications within Vietnam and blocks and deletes
Top ISPs have announced major plans to contribute to the fight against child pornography. Big tech companies are engineering software and technology to detect and protect children from being exploited. For example, Google engineered software to track child pornography in collaboration with the National Centre for Missing and Exploited Children (“NCMEC”). Similarly, Microsoft released a “PhotoDNA” technology in 2009 to automatically identify child pornography and stop them from being redistributed. Furthermore, Apple announced plans to scan iPhones for child pornography. Some online content it doesn’t like. See also Vietnam: Facebook and Google ‘complicit’ in censorship, BBC NEWS (Dec. 1, 2020), archived at https://perma.cc/9N7R-V8H7 (explaining Vietnam’s reputation for restricting freedom of speech by strictly censoring the Internet). See also Freedom on the Net 2019 Saudi Arabia, FREEDOM HOUSE (Nov. 21, 2021), archived at https://perma.cc/6AWR-V69B (giving an overview of the restrictive efforts Saudi Arabia has made in order to censor the Internet). The Saudi Arabian government maintains control over the Internet infrastructure and blocks what it considers harmful, illegal, or anti-Islamic content. Id.  

80 See Jake Wallis Simons, Google is Taking A Stand Against Child Porn, BUS. INSIDER (June 17, 2013), archived at https://perma.cc/V769-6C3Z (observing that Google’s corporate values have led the company to set up a 1.27million-dollar fund to create tools to combat child pornography). But see Adam Walser, Sheriff says tech companies not doing enough to stop child porn, ABC (Nov. 10, 2021), archived at https://perma.cc/92MX-W4MA (noting that 65.4 million images of child pornography were identified in 2020). The local Sheriffs found suspects of child pornography that originated from counties all over the world. Id.  

81 See Bajak & Ortutay, supra note 74 (announcing Apple’s plans to scan the iCloud for child pornography).

82 See Maggie Shiels, Google tackles child pornography, BBC NEWS (Apr. 14, 2008), archived at https://perma.cc/4TPV-DSTK (commenting on Google’s software program to help track child sexual abuse material in partnership with the National Centre for Missing and Exploited Children).  

83 See Sarah Perez, Why The Gmail Scan That Led to A Man’s Arrest For Child Porn Was Not A Privacy Violation, TECHCRUNCH (Aug. 6, 2014), archived at https://perma.cc/5V7N-XAQG (explaining how Google tipped off authorities after running a scan on a suspected criminals Gmail account in which illegal images were found). The nature of the discovery was argued to be an invasion of privacy, but others argued that no human actually reads the personal emails, rather it is an automated scan for keywords and phrases. Id. See also Help stop the spread of child exploitation, MICROSOFT (Nov. 20, 2021), archived at https://perma.cc/TRN7-Z9G2 (explaining how Microsoft’s PhotoDNA technology works and how it has donated the technology to the NCMEC).

84 See Bajak & Ortutay, supra note 74 (unveiling plans to detect child pornography by scanning images before they are uploaded to the iCloud). The system will only flag images that are already known in the center’s database ensuring parents’ innocent photos of their child bathing will not be detected. Id. Major concerns are argued about governmental abuse in over Surveillance. Id. See generally Child Sexual Abuse Material (CSAM), supra note 61 (stating, “[t]o date, over 1,400 companies are
praise these protective measures, but many consumers feel their privacy rights are being compromised.\textsuperscript{85} Tech companies are able to evade these concerns and the duty to regulate or monitor their services as Section 230 of the CDA provides ISPs with enormous protection and freedom.\textsuperscript{86}

2. Child Pornography Persists Despite International Efforts

Despite the increase in global laws aimed to protect children from child pornography there are reported countries that still do not consider child pornography a crime.\textsuperscript{87} The International Centre for Missing & Exploited Children analyzed child pornography laws and has found that a number countries have no legislation directly addressing the problem of child pornography.\textsuperscript{88} Unfortunately, no

\textsuperscript{85} See Olivia Solon, \textit{Inside the surveillance software tracking child porn offenders across the globe}, NBC News (July 17, 2020), archived at https://perma.cc/7W69-3XJU (describing how tech companies who are introducing software to track child porn across the globe are facing growing privacy concerns from users). \textit{But see} MODEL LEGIS. \& GLOB. REV., \textit{supra} note 63, at 12 (arguing that ISPs should be allowed to use tools and mechanism to protect children from online sexual abuse). ISPs with tools like PhotoDNA can proactively detect illegal content and speedily remove the material reducing further distribution. \textit{Id.}

\textsuperscript{86} See Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) (finding there needs to be incentives for service providers to regulate content). \textit{See} MODEL LEGIS. \& GLOB. REV., \textit{supra} note 63, at 5 (reporting 51 countries do not define child pornography and 38 do not criminalize the knowing possession of child porn, regardless of intent to distribute). There has been in increase in countries that now have sufficient legislation in place to combat child pornography, but the report suggests this is not enough. \textit{Id. See also} Despite Increase in Global Child Protection Laws Many Countries Still Do Not Consider Child Pornography A Crime, INT’L CTR. FOR MISSING & EXPLOITED CHILD. (Nov. 20, 2021), archived at https://perma.cc/X2AY-M6SJ (determining the problem of child pornography is still an issue despite the new laws enacted). There has been an increase in the number of countries that have created new laws, however there are still 53 countries that still do not consider child pornography a crime. \textit{Id.}

\textsuperscript{87} See Rajaratnam, \textit{supra} note 72 (compounding the problem of child pornography is the lack of legislation internationally to prohibit its production and spread). Out of the countries that had legislation in place the report found the laws were unsuccessful in dealing with the distribution of child pornography efficiently. \textit{Id.}
region of the world is immune from criminals who seek to exploit children through child pornography, making this a global issue.  

C. Actual Knowledge of Illegal Activity

European nations, Canada, and most other countries do not have analogous statues to United States’ Section 230. A reason for this is most prominent online services, like Google, Microsoft, and Facebook are based in the United States, which has created a need for laws that other countries have not yet found necessary. In the two decades since its creation, Section 230 has become a common legal defense for websites attempting to deflect liability for child pornography posted by their users. ISPs are not being held responsible for the content a user posted even when their platforms are used to share child pornography.

Under the CDA, even when the Internet service providers have actual knowledge of illegal activity such as child pornography, there is no statutory or common law authority to compel ISPs to remove

89 See Child Pornography, supra note 14 (acknowledging the availability of child pornography on the Internet and the many sophisticated methods offenders use to evade law enforcement detection). Further stating, “[t]hese online communities have promoted communication and collaboration between child pornography offenders, thereby fostering a larger relationship premised on a shared sexual interest in children.” Id.

90 See Section 230 of the Communications Decency Act, ELEC. FRONTIER FOUND. (Nov. 20, 2021), archived at https://perma.cc/6HAL-LJ4R (noting that most other countries do not provide ISP with the type of immunity the United States gives to protect the growth of the Internet).

91 See id. (determining although Section 230 if not found elsewhere in the world it is needed in the United States because “most prominent online services are based in the United States.”).

92 See M.A. v. Vill. Voice Media Holdings, 809 F. Supp. 2d 1041, 1048–50 (E.D. Mo. 2011) (finding that under Section 230 of the CDA, Backpage.com was not legally liable for sexual advertisements of a 14-year-old girl who was being trafficked). Section 230 immunity could not be defeated by Backpage.com because posting instructions on how to better promote the advertisement, by itself, is not enough if the website did not post the ad itself). Id. See also Doe v. Backpage.com, LLC, 817 F.3d 12, 18 (1st Cir. 2016) (finding that Section 230 of the CDA provided legal immunity to Backpage.com for advertisements for escorts who were all minors at the time who were victims of sex trafficking); Backpage.com, LLC v. Cooper, 939 F. Supp. 2d 805, 823 (M.D. Tenn. 2013) (finding that the argument that Section 230 of the CDA pre-empted a state law).

93 See Maria Lourder Asención, Further Article: Classified Websites, Sex Trafficking, and the Law: Problem and Proposal, 12 INTERCULTURAL HUM. RTS. L. REV 227, 246 (affirming that Section 230 provide full immunity to ISPs as they published content by other).
offending material.\textsuperscript{94} For example, Craigslist in 2009 was the largest source for prostitution, but the Supreme Court held that under Section 230, Craigslist was immune from the wrongs posted by their users.\textsuperscript{95} Similarly, in \textit{Doe v. Bates}, the Court held that while there was child pornography taking place in a chat hosted by Yahoo, Congress did not intend to deter the Internet service providers, but instead those who created the illegal material.\textsuperscript{96} Big tech platforms have been exempt from civil suits related to child pornography due to Section 230, effectively creating a safe haven for child pornography.\textsuperscript{97} Up until now, the U.S. lacked civil or criminal cases against websites for hosting illegal content on their sites.\textsuperscript{98}

IV. ANALYSIS

From online banking to online shopping, the world has come to know the Internet as second nature for convenience, which has made

\textsuperscript{94} See Kuzma, \textit{supra} note 75, at 36 (explaining that even if an ISP does find suspicious material, it is not required to remove the post even if informed by law enforcement that the post involves child pornography).

\textsuperscript{95} See Dart \textit{v. Craigslist}, Inc., 665 F. Supp. 2d 961, 962–67 (N.D. Ill. 2009) (detailing how the Sheriff of Cook County sought to take down Craigslist, which was the largest source of prostitution in the country, but the court ruled if Craigslist “passively displays content that is created entirely by third parties, then it is only a service provider with respect to that content.”).

\textsuperscript{96} See Doe \textit{v. Bates}, 35 Media L. Rep. 1435, 1435 (E.D. Tex. 2006) (explaining how the plaintiff sued Yahoo for hosting pornography on its chat group and was unsuccessful).

\textsuperscript{97} See Birnbaum, \textit{supra} note 50 (explaining that “reports of child sexual exploitation online have skyrocketed in recent years, as criminals use popular platforms including Facebook, Twitter and YouTube to spread images and videos of minors in violation of federal law.”). These big tech companies have been insulated from victims of child pornography suing them based on the protections provided by Section 230. \textit{Id. The Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020} (EARN IT) could address these concerns by taking away the some of the immunity provided by Section 230. \textit{Id.}

\textsuperscript{98} See Anirudh Krishna, \textit{Internet.gov: Tech Companies as Government Agents and the Future of the Fight Against Child Sexual Abuse}, 109 CALIF. L. REV. 1581, 1582 (2021) (examining tech companies’ efforts in addressing the problem of child pornography). “Unfortunately, the existing legal framework and current efforts by tech companies have not been nearly enough to effectively combat the exponential spread of CSAM online.” \textit{See also} Burnitis, \textit{supra} note 42, at 149 (explaining how FOSTA extended beyond amending and clarifying Section 230 by creating criminal and civil liability for ISPs which intend to promote or facilitate prostitution on their website).
child pornography more accessible than ever.\textsuperscript{99} Although Section 230 is responsible for the development of the Internet, it also has provided a shield for online platforms to escape liability, creating an unsafe environment for users.\textsuperscript{100} The combination of the significant technological changes since 1996 and the expansive interpretation of Section 230 has left ISPs immune from illegal activity on their services.\textsuperscript{101} This outdated Internet law needs to be reformed and realigned to the realities of the modern Internet, while still supporting users freedom of speech.\textsuperscript{102}

\textbf{A. Big Tech has Made Section 230 Outdated}

Section 230 was meant to nurture emerging ISPs and incentivize them to regulate harmful content online, but in the twenty-six years since Section 230 was created, ISPs have gained little incentive to address illicit activity such as child pornography.\textsuperscript{103} Although Section

\textsuperscript{99} See Dickinson, supra note 41, at 369 (illustrating the state of the Internet when Section 230 was created). “Online banking was virtually unheard of, and almost all banking was still conducted at brick-and-mortar locations.” Id. Even a bank’s website only had their hours of operation, typically with no online banking functionality. Id. See Frangoul, supra note 28 (listing ways that the Internet has transformed our lives). See Noeth, supra note 26, at 768 (describing how Congress found that the Internet was starting to flourish in 1996 with hardly any government regulation). “The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.” Id. Americans were beginning to rely on the Internet, and Congress reasoned that imposing liability on ISPs would threaten the development of the industry and create disincentives for self-regulation, thus enacting Section 230. \textit{Id.}

\textsuperscript{100} See Barr, supra note 4 (articulating that Section 230 immunity needs to be reformed to incentivize ISPs to police the illegal content shared on their platforms). See also Dickinson, supra note 41, at 369 (explaining how “[w]hen Section 230 was enacted in 1996, less than eight percent of Americans had access to the internet, and almost all of them, access was through painfully slow dial-up connection.”). Google and email had not even been invented yet, and online banking was unheard of. \textit{Id.}

\textsuperscript{101} See Esposito, supra note 2, at 548 (discussing the growth rate of the Internet in America compared to the unexpected international growth). “At its conception, the Internet was not intended to be a multipurpose, global system that it is today.” \textit{Id.}

\textsuperscript{102} See MALBY et al., supra note 58, at 55 (suggesting that legislation needs to keep pace with technological innovations). While many countries have updated their computer-crime laws it is important to revise existing laws to be flexible in a way that can adapt to the fast-moving technological advancements. \textit{Id.} “Laws and international cooperation mechanisms must also address the need for timely access to information across national boundaries.” \textit{Id.}

\textsuperscript{103} See Peterson, supra note 1, at 765(demonstrating that Section 230 has strayed from its original intent of making the internet safe by completely removing any incentive for ISPs to prevent child pornography from being distributed). See also
230 was supposed to encourage monitoring of the Internet while still enabling growth, Congress instead has found that websites have become reckless in allowing illegal content to be shared and did little to prevent it.\textsuperscript{104} Tech companies are some of America’s largest and most valuable companies and have become an essential role in how Americans communicate and engage in commerce.\textsuperscript{105} The realities of the modern Internet is that ISPs no longer function as simple forums for posting third-party content, but instead use a sophisticated algorithms to promote content and connect users.\textsuperscript{106} ISP no longer need to be nurtured because the tech industry has become very well established, making the vast immunity no longer necessary as ISPs would not be unduly burdened by making the internet safer for users.\textsuperscript{107}

\textbf{B. Not Abandoning Section 230, Rather, Making it Appropriate for the Decade}

The challenge with removing the Section 230 immunity is that it would open ISPs up to enormous amounts of litigation because users would freely be able to sue for any and all cases of possible defamation.\textsuperscript{108} Disrupting the business of ISPs in a dramatic way could have effects on international economics and a full range of other human social activity if ISPs were not able to conduct their business

\textsuperscript{104} See Burnitis, \textit{supra} note 41, at 149 (stating that Congress found websites had become reckless in allowing prostitution to occur on their websites, therefore FOSTA was needed to clarify Section 230 of the CDA).

\textsuperscript{105} See \textit{Key Takeaways and Recommendations, supra} note 4, at 2 (expressing the valuable role the Internet and social media have played in the development of the nation, and how Americans communicate and engage in commerce).

\textsuperscript{106} See Dickinson, \textit{supra} note 41, at 348 (clarifying that in 1996 the Internet was primarily for content distribution, but today the Internet operates in a much more expansive real-world sense where users can accomplish any physical-world task on an app).

\textsuperscript{107} See \textit{Key Takeaways and Recommendations, supra} note 4, at 2 (asserting that online platforms do not need to be nurtured like in 1996 when the Internet was first taking off; rather, there is a need to tailor changes to their immunity because it would not impose an undue burden on such tech giants).

\textsuperscript{108} See id. at 14 (explaining how experts in the tech industry are concerned about changes to Section 230 leading to frivolous litigation which would place a burden on them).
as usual. Rather than creating a new framework for the Internet, creating carve outs in the current framework would be more feasible. If ISPs were held accountable for harboring child pornography there would be a greater incentive for ISPs to initiate practices of removing child pornography from their services. Focusing on ISPs policing practices in general rather than their response to a specific piece of child pornography would encourage a continuous system of preventing the spread of child pornography.

From the EARN IT Act, a knowledge standard was set: when ISPs have direct and clear knowledge that their platforms are involved in the distribution of child pornography, they will be held accountable. A knowledge standard can imply an “ignorance is bliss” standard for companies wanting to avoid liability by not monitoring their

---

109 See Dickinson, supra note 41, at 385 (expressing that while momentum is building to reform Section 230, some fear that altering the protections offered to ISPs could “endanger the United States’ position as a worldwide innovation leader.”). Because Section 230 is so broad in granting immunity, any change would cause a significant ripple effect in the tech industry by giving them more obstacles to remain compliant with certain new regulations. Id.

110 See KEY TAKEAWAYS AND RECOMMENDATIONS, supra note 4, at 11 (highlighting the need to reform Section 230 while drawing attention to how it is important to preserve the core of Section 230’s immunity for defamation).

111 See Dickinson, supra note 41, at 384–85 (proposing to amend “Section 230 to require that an entity take ‘reasonable steps to prevent or address unlawful uses of its services’ to be eligible for immunity.”). “Making immunity contingent on entities’ practices as a whole could encourage industry organizations to develop best practices for policing online content and foster a business culture more attuned to the harms caused by the technologies they deploy.” Id. at 385.

112 See KEY TAKEAWAYS AND RECOMMENDATIONS, supra note 4, at 3 ( Recommending a reform Section 230 to incentivize online platforms to take actions against illicit content online). See also Dickinson, supra note 41, at 385 (proposing that Section 230 should be reformed to focus on an ISPs policing practices rather that is response to the particular piece of content that precipitated a plaintiff’s alleged harms).

Reasonable policing practices could be defined either abstractly, via a reasonableness standard like that proposed by Citron and Wittes, or could be particularized via statutory or regulatory mandate. A reasonableness standard would provide courts flexibility to adapt Section 230 for new contexts and different types of entities, whereas particularized regulations would provide entities greater certainty ex ante regarding whether their practices would qualify them for immunity.

Id.

113 See Birnbaum, supra note 50 (explaining that the EARN IT Act would have left online platforms liable for a broad set of federal civil penalties if they ‘recklessly,’ rather than ‘knowingly,’ provided a service that was used to distribute child sexual abuse material.”).
platforms. If companies are actually incentivized to adhere to the best practices set by the EARN IT Act, it is more likely they will comply. Although, when the incentive is for tech companies to scan private data, consumers raise concerns for their rights to privacy being invaded by these data scans. The goal is not to take constitutional rights, but to have tech companies take responsibility of what is on their platforms.

C. The Burden to Screen for Child Pornography is No Longer a Burden

Previously, courts have held ISPs immune to content from a third-party user because to do otherwise, meaning to hold them accountable for obscene material from a user, would impose too large of a burden. In the last two decades of rapidly advancing technology,

114 See Key Takeaways and Recommendations, supra note 4, at 2 (explaining how “[p]latforms therefore faced a dilemma: They could try to moderate third-party content but risk being held liable for any and all content posted by third parties, or choose not to moderate content to avoid liability but risk having their services overrun with obscene or unlawful content.”).

115 See Birnbaum, supra note 50 (expressing that the flaws in the EARN IT Act would make it harder to get rid of child pornography without violating Fourth Amendment rights to privacy). “’The EARN IT Act remains a deeply flawed proposal that would make it harder for IA member companies to rid the internet of [child sexual abuse material] and protect the most vulnerable online,’ said Mike Lemon, the senior director of federal government affairs with the Internet Association.” Id.

116 See Zakrzewski, supra note 49 (addressing a Bill to protect children online Senator Richard Blumenthal stated “lawmakers incorporated these concerns into revisions, which prevent the implementation of encryption from being the sole evidence of a company’s liability for child porn. But he said lawmakers wouldn’t offer a blanket exemption to using encryption as evidence, arguing companies might use it as a ‘get-out-of-jail-free card.’”). Social media sites and certain tech companies have major flaws, and these companies need to partner with authorities to create “safe spaces online.” Id.

117 See Stern, supra note 56 (stating the goal of the EARN IT Act is to get ISPs and social media companies to take responsibility of the content users post on their platforms).

118 See Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) (determining the immunity ISPs have for wrongs committed by their users under Section 230). ISPs have no obligation to remove tortious material, to prevent the reposting of objectionable materials, or to help victims track down the primary wrongdoers. Id. at 331. By applying the rational of Zeran, ISPs may have knowledge and warning about the existence of child pornography and still be immune from civil suits under Section 230. Id. at 330. See also Doe v. Bates, No. 5:05-CV-91-DF-CMC, 2006 U.S. Dist. LEXIS 93348, at *12 (E.D. Tex. Dec. 27, 2006) (extending the immunity for Yahoo! so they could not be sued by the parents of a child who Yahoo! allegedly
we have entered a time where it is no longer unfeasible for ISPs to police their services.\footnote{119 Apple, Google, Microsoft, and other huge tech companies have proved they are capable of preventing child pornography and there is software available to do so.} For example, ISPs and social media sites that provide services to millions could not respond to all content complaints daily, but they may deploy software to detect and remove child pornography that has previously been deemed illegal.\footnote{120 See KEY TAKEAWAYS AND RECOMMENDATIONS, supra note 4, at 2 (articulating the dramatic changes in the 25 years since the creation of Section 230). Several online platforms have transformed into some of the nation’s largest and most valuable companies, and today’s online services bear little resemblance to the rudimentary offerings in 1996. Platforms no longer function as simple forums for posting third-party content, but instead use sophisticated algorithms to promote content and connect users.}

\textit{Id.} See Bajak & Ortutay, supra note 74 (announcing Apple’s plans to scan the iCloud for child pornography). See also Shiels, supra note 82 (commenting on Google’s software program to help track child sexual abuse material in partnership with the National Centre for Missing and Exploited Children). See also Perez, supra note 83 (explaining how Google has the ability to help authorities stop the spread of sharing illegal images by scanning Gmail accounts). See also Help Stop the Spread of Child Exploitation, supra note 83 (explaining how Microsoft developed PhotoDNA technology which they donated to the NCMEC). But see Solon, supra note 85 (describing how tech companies who are introducing software to track child porn across the globe are facing growing privacy concerns from users). See also MODEL LEGIS. & GLOB. REV., supra note 63, at 12 (arguing that ISPs should be allowed to use tools and mechanisms to protect children from online sexual abuse). ISPs with tools like PhotoDNA can proactively detect illegal content and speedily remove the material, reducing further distribution. \textit{Id.} See Dickinson, supra note 41, at 385 (explaining different strategies to provide standards to allow courts flexibility to adapt Section 230 for new contexts and different types of entities). “The duty of care would vary by entity type and size and require more of online entities as technology improves.” \textit{Id.} at n.221. “[W]hereas particularized regulations would provide entities greater certainty ex ante regarding whether their practices would qualify them for immunity.” \textit{Id.} at 385. See MODEL LEGIS. & GLOB. REV., supra note 63, at 12 (addressing the need for industry responsibility by advocating that companies should be allowed to deploy tools and mechanisms to scan their platforms to identify and tack down child pornography). “ISPs also may employ filtering and/or blocking technologies to impede access to [child pornography]. Tools like PhotoDNA can detect [child pornography] being
D. First Amendment Issues Shouldn’t Prevent the Eradication of Child Pornography

The major issue with increase policing and monitoring of content online is whether the First Amendments freedom of speech is jeopardized.\textsuperscript{122} Allowing and incentivizing ISPs to remove content shared by a third party can lead to over policing and invading individuals right to share, advocate, and express themselves online.\textsuperscript{123} Currently, Section 230 protects ISPs both when they leave material up and when they take it down.\textsuperscript{124} Proposals have suggested that the protection provided by Section 230 should only be granted when systems are in place to take down child pornography.\textsuperscript{125} By creating a carve out for ISPs to be given Section 230 immunity when they have a system in place to track child pornography it will effectively incentivize ISPs who wish to remain immune from liability of Freedom of Speech violations.\textsuperscript{126} This carve out would still uphold freedom of speech for legally shared material while incentivizing the removal of child pornography.\textsuperscript{127}

\textsuperscript{122} See Kuzma, supra note 75, at 40–41 (articulating certain constitutional issues regarding First Amendment protections). “[T]he Internet is likely a unique aspect of commerce that demands national treatment.” Id. at 41.
\textsuperscript{123} See Bambauer, supra note 24 (calling proposed reforms to Sections 230 “content-moderation regimes” as they aim to strip ISPs of their liability protection).
\textsuperscript{124} See Dickinson, supra note 41, at 351–52 (explaining how when Section 230 was created it treated ISPs as publishers because that was essentially the role of ISPs at the time). Congress treated ISPs as purely an “information content provider” and therefore they cannot be held liable for any on the content they facilitate because they are merely the publisher. Id.
\textsuperscript{125} See Birnbaum, supra note 50 (explaining that if the EARN It Act is amended it would require ISPs to become serious in taking down child pornography from their platforms).
\textsuperscript{126} See KEY TAKEAWAYS AND RECOMMENDATIONS, supra note 4, at 14 (expanding on issues in need for legislative reform including “reforms to better incentivize online platforms to address illicit content.”). Section 230 currently is designed to facilitate illegal conduct but retain immunity from liability. Id. “When it comes to unlawful content related to federal crimes like child exploitation, . . . however, it is far less clear that we should be concerned about chilling such activity, and instead should be more concerned about halting such dangerous behavior.” Id. at 17.
\textsuperscript{127} See New York v. Ferber, 458 U.S. 747, 756–58 (1982) (finding that child pornography is not protected by the First Amendment because our society has an interest in protecting children from sexual abuse). See also Osborne v. Ohio, 495
E. Combating an International Child Pornography Issue with Uniformity

The ability to share child pornography across the globe in mere seconds makes determining the volume of child pornography difficult. A reason for this is that there is no international governing body in place to monitor and police such activity. While there are many instruments that address how to decrease the availability of child pornography on the Internet, there are still gaps between the national and international efforts. The gap in defining who is a child becomes an issue when some countries find obscene picture of a consenting thirteen-year-old legal, and other countries would find that same picture criminal. The definition of a child is a critical issue in providing protection for children at an international level which proves there needs to be uniformity in international laws regarding child pornography. Many countries fail to recognize a cognizable

U.S. 103, 107 (1990) (extending the holding of Ferber from child pornography to private possession of child pornography).

128 See Dickinson, supra note 41, at 382–83 (highlighting how recent proposals suggest removing immunity protections from the most egregious crimes online). [S]uch proposals focus on stripping immunity from the most egregious offenders: those online entities that intentionally facilitate criminal behavior. For example, a recent Department of Justice review of Section 230 concluded that a “Bad Samaritan” carve out should be added to the statute to ensure that online entities that purposefully solicit “third parties to sell illegal drugs to minors, exchange child sexual abuse material,” or engage in other unlawful activities through their platforms “do not benefit from Section 230's sweeping immunity at the expense of their victims.”

Id. (quoting Department of Justice)

129 See Kalim, supra note 59, at 435 (discussing the depth of the problem on measuring the prevalence of child pornography). Because there is no governing body to monitor child pornography, online data must be collected from prosecutors. Id.

130 See id. at 432 (explaining that countries differ on a standard measurement or definition of a child, “which makes producing a neutral standard to gauge Internet child pornography difficult.”). Some countries define a child by when they are legally able to consent to sex or the legal age to vote. Id. A few even determine a child based on the age to legally get married. Id. at 433.

131 See Kalim, supra note 59, at 438–39 (advocating that a child, for the purposes of child pornography, should be considered anyone under the age of eighteen and that ability to give legal sexual consent should not determine when pornography is child pornography). The legal age of sexual consent varies by country which makes it difficult to be consistent in the protection of children. Id. at 433.

132 See Malby et al., supra note 58, at 46 (explaining the need for cooperation between law enforcement in nineteen different countries when investigating fifty-five suspects on social media trading child pornography).
standard of measurement or definition of the term "child," which makes producing a neutral standard to gauge Internet child pornography difficult.133

The substantial variations in definitions, penalties and interpretations of laws surrounding child pornography prevents the end of child pornography.134 Creating a single, unitary framework to govern all internet conduct comes with major concerns and difficulties.135 For example, PhotoDNA has been helpful for law enforcement in preventing child pornography, but many countries prohibit the use of such invasive evidence.136 America, being a world leader in technological innovations, has an opportunity to lead in preventing child pornography.137 Withholding ISPs immunity based on whether they have implement systems to scan for child pornography would add a strong incentive for ISPs to take steps in contributing to the eradication of child pornography.138 It is ineffective to assume ISPs voluntarily monitor the content on their platforms;

133 See Kalim, supra note 59, at 432–49 (elaborating on the depth of the issue regarding the variations in international definitions, protections of children, punishments of offenders, and regulations of child pornography which make it more difficult to prevent the spread of child pornography).

134 See MODEL LEGIS. & GLOB. REV., supra note 63, at 33 (describing the measures to protect children as building blocks helping to move in the direction of enabling countries to frame child protections as a priority). The report suggests how child pornography should be defined, the age of a child, and how knowing possession of child pornography should be criminalized. Id. at 7–8. “A holistic and uniform approach is the most effective means of combating the sexual exploitation of children because it allows for consistency in criminalization and punishment … and it improves overall law enforcement efforts at the national and international levels.” Id. at 20.

135 See Dickinson, supra note 41, at 385 (highlighting the difficulties in creating a singular framework to govern Internet conduct). “[T]he risk of increased uncertainty and compliance costs associated with a more flexible rule; and the risk of increased litigation expenses in the technology industry.” Id.

136 See MALBY ET AL., supra note 58, at 46 (advocating that “[s]uch data is essential to support cases that require proof that the children depicted in [child pornography] material are indeed real children and not the product of digital animation.”).

137 See Dickinson, supra note 41, at 382 (stating “[f]or decades now, Section 230 has been treated as sacred. Industry leaders, joined by prominent legal scholars, have presented a united voice, warning that changes to the statute would undermine the American tech industry and the internet as we know it.”).

138 See Burnitis, supra note 41, at 166 (arguing in order for America to be effective in protecting children from the evils of the Internet there needs to be legislation in place that is well tailored to these issues on child pornography). “Only with effective, well-tailored, and survivor-focused legislation can America truly begin to win the war against human trafficking.” Id.
rather if ISPs are incentivized to regulate their services, it is more likely they will comply.

V. CONCLUSION

As the Internet and technology have advanced in the last two decades, regulations for the Internet and monitoring software tools should progress along with the rapid pace of the tech industry. While it would be unfathomable to require ISPs to manually monitor the content posted by third parties, it is reasonable to expect the advance state of technology today to provide systems to makes our Internet spaces safer for children. There is a demand for international uniformity in combating child pornography, which includes a determination of the age of a child. For the purposes of accepting and enforcing international obligations, countries will need to be willing to identify when legal protection from Internet child pornography and the harms associated with its production would be assented to and implemented. Requiring platforms to provide users with mechanisms to flag unlawful child pornography may be the balance needed to protect privacy rights while also clearing the Internet of child pornography.