South Carolina Journal of International Law and Business

Volume 21 | Issue 2 Article 5

2025

The Dark Side of the Internet: The Facilitation of CSAM by Social Media Companies and What Should Be Done about It

Megan Holderness

THE DARK SIDE OF THE INTERNET: THE FACILITATION OF CSAM BY SOCIAL MEDIA COMPANIES AND WHAT SHOULD BE DONE ABOUT IT

By Megan Holderness

I. INTRODUCTION

The internet has changed the way we interact with the world—a fact even Congress has recognized.[1] While definitions of social media are broad and evolving, they can be summarized as "internet-based channels that allow users to opportunistically interact and selectively self-present, either in real-time or asynchronously, with both broad and narrow audiences who derive value from user-generated content and the perception of interaction with others."[2] Today, social media platforms boast an estimated 4.9 billion users worldwide in 2023,[3] and the social networking industry is worth approximately $139 billion.[4]

However, the rise of social media comes with the rise of crimes committed on social media platforms. Some of these crimes include cyberstalking, harassment, hacking, phishing, identity theft, fraud, and drug, gun, and human trafficking.[5] Perhaps one of the most harmful and exploitative of crimes facilitated by social media sites is the sharing of child sexual abuse material (CSAM). Formerly known as child pornography, CSAM is statutorily defined under federal law[6] and includes material depicting anyone under the age of eighteen.[7] Since as recently as 2016, the term "CSAM" has been preferred instead of "child pornography." Pornography is generally

---

[1] "The Congress finds the following: (1) 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. (2) These services offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops. (3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity. (4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation. (5) Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services." 47 U.S.C. § 230.

[2] Caleb T. Carr & Rebecca A. Hayes, *Social Media: Defining, Developing, and Divining*, 23 ATL. J. OF COMMC'N 50 (2015).

[3] Belle Wong, *Top Social Media Statistics and Trends of 2024*, FORBES, (last updated May 18, 2023), https://www.forbes.com/advisor/business/social-media-statistics/.

[4] Alex Petridis, *Social Networking Sites in the US - Market Research Report (2014-2029)*, IBIS WORLD, (last updated Sept. 2024), https://www.ibisworld.com/united-states/industry/social-networking-sites/4574/).

[5] Jill Harness, *The Most Common Crimes Committed on Social Media*, VISTA CRIM. L. (Jan. 18, 2021), https://vistacriminallaw.com/common-social-media-crimes/.

[6] "[C]hild pornography" means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where – (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct." 18 U.S.C. § 2256(8) (Supp. 2009); "Except as provided in subparagraph (B), "sexually explicit conduct" means actual or simulated— (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the anus, genitals, or pubic area of any person; (B) For purposes of subsection 8(B) [(8)(B)] of this section, "sexually explicit conduct" means— (i) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (ii) graphic or lascivious simulated; (I) bestiality; (II) masturbation; or (III) sadistic or masochistic abuse; or (IV) graphic or simulated lascivious exhibition of the anus, genitals, or pubic area of any person…" 18 U.S.C. § 2256(2) (Supp. 2009).

[7] 18 U.S.C. § 2256(1) (Supp. 2009).

generated by adults who have consented to the recording of their sexual acts. However, children cannot consent to sex, or the recording and distribution of their abuse depicted in photos, videos, or other materials. Instead, CSAM is evidence of sexual abuse endured by children and should be referred to as such.[8] In the United States, there are a number of state and federal laws which ban creating, sharing, possessing, and distributing CSAM.[9] It is also banned in most countries around the world, given the egregious nature of these crimes and the life-long effects they have on innocent children who are victimized.[10]

Despite the alarming amount of CSAM on social media platforms, the government has required little of these companies to detect and remove such content. Meanwhile, social media companies have done little, if any, to help solve the problem on their own. While social media companies should do more, they will only do as much as is required of them. Thus, the government needs to take the reins. This paper argues that the government should pass proposed legislation, impose an affirmative duty on social media companies to monitor their platforms for CSAM, and require these companies to implement artificial intelligence (AI) programs more effectively to detect and remove CSAM.

II. THE PROBLEM OF CSAM ON SOCIAL MEDIA

a. Development of Social Media

Shortly after the invention of the internet in 1983,[11] social media sites began popping up on the platform. Digital communication companies such as CompuServe, America Online (AOL), and Prodigy offered real-time messaging unlike anything before.[12] In 1997, the first social media network as known today came on the market: SixDegrees.[13] The following years brought some of the most recognizable and influential social media sites: Friendster in 2001, LinkedIn in 2002, MySpace in 2003, Facebook in 2004,[14] YouTube[15] and Reddit in 2005, Twitter (now X) in 2006,[16] WhatsApp in 2009,[17] Instagram in 2010, Snapchat in 2011, and TikTok in 2016.

Social media networks were initially invented to connect family, friends, and other individuals on a digital platform that could be accessed anywhere in the world. Like-minded communities online formed to foster connection and facilitate communication. While originally

---

[8] *What Is Child Sexual Abuse Material (CSAM)*, RAINN (Aug. 25, 2022), https://rainn.org/news/what-child-sexual-abuse-material-csam [hereinafter *What is CSAM*].
[9] *See* 18 U.S.C. §§ 1466A, 2251–2253.
[10] *INHOPE Global CSAM Legislative Overview 2024*, INHOPE, https://inhope.org/EN/articles/inhope-global-csam-legislative-overview-2024.
[11] *A Brief History of the Internet*, ONLINE LIBR. LEARNING CTR., https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml.
[12] *The Evolution of Social Media: How Did It Begin, and Where Could It Go Next?*, MARYVILLE UNIV. (May 28, 2020), https://online.maryville.edu/blog/evolution-social-media/.
[13] Esteban Ortiz-Ospina, *The Rise of Social Media*, OUR WORLD IN DATA (Sept. 18, 2019), https://ourworldindata.org/rise-of-social-media.
[14] *Evolution of Social Media*, *supra* note 12.
[15] William L. Hosch, *YouTube*, BRITANNICA, https://www.britannica.com/topic/YouTube (last updated Dec. 19, 2024).
[16] *Evolution of Social Media*, *supra* note 12.
[17] Roland Martin, *WhatsApp*, BRITANNICA, https://www.britannica.com/topic/WhatsApp (last updated Feb. 19, 2025).

social media sites were accessed via laptop and desktop computers, the dawn of the smartphone revolutionized their use. The Apple iPhone launched in 2007, which expanded the use of social media to a mobile platform. Further technological developments, such as high-quality in-phone cameras, shifted these platforms to be more photo- and video-oriented.[18] However, social media is no longer simply used for communicating with friends or connecting to compatible strangers. In the modern day, social media platforms are powerful tools to advertise, grow businesses, access information, and influence the political climate. It has transformed how we interact with the world.

With the broad reach of social media, that transformation has been widespread and rapid. In 2019, 3.5 billion people of the world's population of 7.7 billion used the internet.[19] Of those 3.5 billion people, more than two-thirds used at least one social media platform.[20] In the United States, about 70% of Americans used social media sites.[21] These numbers have dramatically increased in a short period of time. From 2005 to 2019, the percentage of U.S. adults using social media increased from 5% to 79%. Facebook's global usership rose from 1.5% in 2008 to 30% in 2018.[22]

Facebook is the largest social media company in the world with 3 billion monthly active users globally, including a third of Americans aged thirteen to seventeen.[23] However, other social media platforms are close behind. In 2018, YouTube had 1.9 billion monthly active users, WhatsApp had 1.33 billion in 2017, WeChat and Instagram had 1 billion each, and TikTok had 500 million.[24]

There are age, gender, and socio-economic differences that affect the use of social media, which may vary among platforms. Trends consistently show that young people use social media sites more than the older population. For example, in 2019, 90% of adults aged eighteen to twenty-four of the surveyed group had used YouTube while 38% of adults aged sixty-five and older had used it.[25] Additionally, on average women use social media more than men.[26] Those numbers may also vary by platform, as women used Pinterest more while men used Reddit more in 2021.[27] Furthermore, in wealthy countries, as many as 96% of people aged sixteen to twenty-four are social media users.[28] This may be attributed in large part to the widespread availability of the internet in these countries and greater accessibility to technological devices. With such frequent use comes a lot of time spent on social media sites as well. In 2018, the average social media user in the U.S. spent more than six hours daily on these platforms.[29] While social media can provider

---

[18] *Evolution of Social Media*, *supra* note 12.
[19] Ortiz-Ospina, *supra* note 13.
[20] *Brief History of the Internet*, *supra* note 11.
[21] Matthew Jones, *The Complete History of Social Media: A Timeline of the Invention of Online Networking*, HISTORY COOPERATIVE (Oct. 31, 2024), https://historycooperative.org/the-history-of-social-media/.
[22] *Brief History of the Internet*, *supra* note 11.
[23] Katherine Schaeffer, *5 Facts About How Americans Use Facebook, Two Decades After Its Launch*, PEW RESEARCH CENTER (Feb. 2, 2024), https://www.pewresearch.org/short-reads/2024/02/02/5-facts-about-how- americans-use-facebook-two-decades-after-its-launch/.
[24] Ortiz-Ospina, *supra* note 13.
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.*

a lot of positive material for users, they can also facilitate a lot of negative material as well.

b. History of CSAM

The history of child sexual exploitation is, unfortunately, a long one. In ancient Greece, children as young as twelve years old were forced to enter marriages and sexual relationships with adults.[30] This trend continued throughout time: fourteen-year-old girls were married off in the Roman Empire, seven-year-old girls were made to wed in medieval times, and an adult could legally have sexual relations with girls as young as ten in early nineteenth-century England.[31] Children have been sexualized in art and writings throughout history, as well, including in ancient Greece, ancient Rome, and during the Renaissance.[32] However, the 1826 invention of the camera signaled a turning point in CSAM production.[33] Later, in the 1970s, popular films and magazines portrayed child abuse in media.[34] Initially, this CSAM was expensive, the images were low quality, the chances of being caught were high, and the distribution speed was slow. However, the dawn of the internet has caused a boom in the CSAM market. Today, offenders can easily connect to each other; CSAM is available twenty-four hours per day; and access is often free, anonymous, and instant.[35]

Child sexual abuse is often committed by people the child knows, including family members and trusted adults in their life. Most offenders involved with the possession and distribution of CSAM also commit participatory offenses against these minor victims through grooming, secrecy, and normalization.[36] The statistics regarding CSAM production, distribution, and consumption are alarming. In 2021, online platforms reported almost 30 million cases of suspected child sexual exploitation online to the National Center for Missing & Exploited Children (NCMEC) CyberTipline, including about 85 million photos and videos which constituted CSAM.[37] The ages of these children varied but there are some trends: about 4% showed infants or toddlers, 56% showed prepubescent children, 25% showed pubescent children, and 14% showed children across multiple age groups.[38] Of these, 97% of CSAM victims were girls.[39] Additionally, about 82% of CSAM featured severe abuse. The most severe abuse was more likely to be committed against younger children.[40] The good news is 89% of the more than 252,000

---

[30] Bryce Garreth Westlake, *The Past, Present, and Future of Online Child Sexual Exploitation: Summarizing the Evolution of Production, Distribution, and Detection*, THE PALGRAVE HANDBOOK OF INTERNATIONAL CYBERCRIME AND CYBERDEVIANCE, June 2020, at 5.
[31] *Id.* at 5–6.
[32] *Id.* at 6.
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] Janis Wolak, David Finkelhor, & Kinberly J. Mitchell, *Child-Pornography Possessors Arrested in Internet- Related Crimes: Findings From the National Juvenile Online Victimization Study*, *in* UNIVERSITY OF NEW HAMPSHIRE SCHOLARS' REPOSITORY: CRIMES AGAINST CHILDREN RESEARCH CENTER (2005).
[37] *What is CSAM*, *supra* note 8.
[38] *Id.*
[39] United Nations Office on Drugs and Crime (UNODC), *Background Paper: Towards Zero: An Initiative to Reduce the Availability of Child Sexual Abuse Material on the Internet*, at 6, (2023), https://www.unodc.org/pdf/criminal_justice/endVAC/EGM/EGM_CSAM_Removal_Background_Paper.pdf [hereinafter *UNODC CSAM Paper*].
[40] *Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material: Summary Report*

CSAM URLs reported to the Internet Watch Foundation (IWF)[41] were traced back to the original owners or digital storage spaces, which enabled them to find the offenders' locations.[42]

Troubling data shows that the United States hosts more CSAM than any country in the world.[43] As of 2022, the United States made up 30% of the world's total CSAM URLs.[44] Part of the reason for that is that many CSAM sites have moved their servers to the U.S. in recent years.[45] There may be other nearly unsolvable factors that contribute to this as well: the large population size of the U.S. (337 million people in 2024)[46], the country's hub as the host of the most secure internet servers and data centers in the world, and the overwhelming volume of CSAM for law enforcement to investigate. These circumstances, as well as the availability of the internet, have created the perfect storm for CSAM possession and distribution to thrive.

Victims of CSAM often feel the negative effects of these heinous crimes committed against them long after their victimization. These survivors report feelings of guilt, shame, trouble with adult intimacy and relationships, problems with oversexualized behavior, low self-esteem, alcohol and substance abuse, eating disorders, and mental illnesses such as depression and post-traumatic stress disorder (PTSD).[47] Overwhelmingly, CSAM victims suffer from feelings of powerlessness and embarrassment as they are in constant fear of not only their perpetrators, but also being recognized as they move into adulthood.[48]

c. Social Media Companies' Facilitation of CSAM

The interconnectivity and easy access of social media has led to a global rise in cybercrime committed on these sites. With the internet's expeditious growth in the 1990s and early 2000s, peer-to-peer (P2P) file-sharing sites,[49] social media platforms, and instant messaging have resulted

---

(2018), INTERPOL & ECPAT INTERNATIONAL, https://ecpat.org/wp-content/uploads/2021/05/TOWARDS-A-GLOBAL-INDICATOR-ON-UNIDENTIFIED-VICTIMS-IN-CHILD-SEXUAL-EXPLOITATION-MATERIAL-Summary-Report.pdf.

[41] IWF is based in the United Kingdom and operates in 30 countries. *Internet Watch Foundation*, SAFE ONLINE, https://safeonline.global/internet-watch-foundation-1/.

[42] Rhiannon Williams, *The US Now Hosts More Child Sexual Abuse Material Online Than Any Other Country*, MIT TECHNOLOGY REVIEW (Apr. 26, 2022), https://www.technologyreview.com/2022/04/26/1051282/the-us-now-hosts-more-child-sexual-abuse-material-online-than-any-other-country/.

[43] *What is CSAM*, *supra* note 8.

[44] *UNODC CSAM Paper*, *supra* note 39.

[45] *What is CSAM*, *supra* note 8.

[46] *U.S. and World Population Clock*, UNITED STATES CENSUS BUREAU, https://www.census.gov/popclock/ (last updated Dec. 19, 2024).

[47] *What is CSAM*, *supra* note 8.

[48] United Nations Office on Drugs and Crime (UNODC), *Background Paper: Towards Zero: An Initiative to Reduce the Availability of Child Sexual Abuse Material on the Internet*, at 7, (2023), https://www.unodc.org/pdf/criminal_justice/endVAC/EGM/EGM_CSAM_Removal_Background_Paper.pdf.

[49] "In general, individuals become P2P users by downloading software that connects them to the computers of other users in a network (e.g., Gnutella, BitTorrent, Ares). These other users could be located anywhere in the world. The software allows users to log onto the P2P network and issue requests for and download files from other network users, called peers. Users create shared folders that are accessible to others in the network and use these folders to receive downloaded files and also to share files they possess. Procedures vary somewhat among networks, but in most, users search for electronic files by using keywords, which are broadcast to the network of participating peers." Janis Wolak, Marc Liberatore, & Brian Neil Levine, *Measuring a year of child pornography trafficking by U.S. computers on a peer-to-peer network*, 38 JOURNAL OF CHILD ABUSE & NEGLECT (2014), https://www.sciencedirect.com/science/article/abs/pii/S0145213413003232.

in the prevalence of CSAM online.[50]

In a 2012, the U.S. Sentencing Commission reported to Congress that CSAM offenders use social media to groom minors and solicit CSAM from them.[51] They also emphasized the internet's evolving role in CSAM in the United States:

> Until the late 1970s and early 1980s, child pornography was difficult to find, risky to produce, expensive to duplicate, and required a secure and private storage area. Technological advances since that time have made child pornography much more widely available and reduced the barriers to offending. . . Most child pornography offenders now rely on Internet or Internet enabled technology to access and distribute child pornography . . . Many child pornography offenders rely on P2P networks . . .[52]

The statistics also support these assertions. In the last 15 years, NCMEC has seen a 15,000% increase in CSAM files reported.[53] Almost a million CSAM files were reported on Google, Dropbox, Microsoft, Snapchat, TikTok, X, and Verizon Media. In the fourth quarter of 2020, alone, Meta reported the removal almost 5.5 million CSAM files from their platform.[54] From 2005 to 2019, the development of mobile and digital technology resulted in an increase in offenders sentenced for CSAM production by 422%,[55] which is a sizeable increase but still does not keep up with the rapid rates of CSAM distribution.

In today's world, offenders sometimes gradually escalate inappropriate interactions to soliciting CSAM from minors themselves. Self-generated CSAM is less likely on popular platforms like X or Instagram, but they can occur on any social media site.[56] Through social media networks, offenders build digital relationships of trust in which they groom the minor and normalize sexualization. After building that rapport, offenders suggest, pressure, or trick minors into sending them nude photos, performing sexual acts, or exchanging explicit messages. About

---

[50] Bryce Garreth Westlake, *The Past, Present, and Future of Online Child Sexual Exploitation: Summarizing the Evolution of Production, Distribution, and Detection*, THE PALGRAVE HANDBOOK OF INTERNATIONAL CYBERCRIME AND CYBERDEVIANCE, June 2020, at 6.

[51] *Federal Child Pornography Offenses*, UNITED STATES SENTENCING COMMISSION, at 267, https://www.ussc.gov/sites/default/files/pdf/news/congressional-testimony-and-reports/sex-offense-topics/201212-federal-child-pornography-offenses/Full_Report_to_Congress.pdf.

[52] *Id.* at 71.

[53] Glen Pounder & Rasty Turek, *On Social Media, Child Sexual Abuse Material Spreads Faster Than It Can Be Taken Down*, FAST CO. (July 14, 2021), https://www.fastcompany.com/90654692/on-social-media-child-sexual-abuse-material-spreads-faster-than-it-can-be-taken-down.

[54] *Social Media Is Accelerating the Spread of Child Sexual Abuse Material*, GIVING COMPASS (May 3, 2024), https://givingcompass.org/article/social-media-is-accelerating-the-spread-of-child-sexual-abuse-material (citing Glen Pounder & Rasty Turek, *On Social Media, Child Sexual Abuse Material Spreads Faster Than It Can Be Taken Down*, FAST COMPANY (July 14, 2021), https://www.fastcompany.com/90654692/on-social-media-child-sexual-abuse-material-spreads-faster-than-it-can-be-taken-down).

[55] *Federal Sentencing of Child Pornography: Production Offenses*, UNITED STATES SENTENCING COMMISSION (October 2021), https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2021/20211013_Production-CP.pdf.

[56] David Thiel & Renée DiResta, *Child Safety on Federated Social Media*, STANFORD INTERNET OBSERVATORY, at 8, (July 2023), https://stacks.stanford.edu/file/druid:vb515nd6874/20230724-fediverse-csam-report.pdf.

10% of CSAM was obtained in this way. However, the offenders may not stop at grooming and CSAM solicitation. From there, offenders may engage in sextortion[57] or commit hands-on sexual offenses against the minor.[58]

CSAM can be exchanged on social media sites in a variety of ways. The exchanges may occur via direct messages, chat rooms, private video calls, private channels, file-sharing and purchasing, and even through posts or hashtags.[59] On Snapchat, messages can disappear instantly, and metadata can be hard to retrieve, which makes it more difficult for law enforcement to collect evidence of CSAM creation, possession, or distribution. However, if the content is saved by a user communicating in that chat with another user, the content is still available. Snapchat also offers a story function to broadcast content to "friends" and offers public profiles for users to reach an even wider audience. With so many options on the social media market, consumers can find just about any platform with ease.

It is important to note that social media companies do not just include the big names we may use in everyday life like Facebook, Instagram, or TikTok. For example, Gnutella is a file-sharing network in which people can post and access digital files. In a one-year span, from 2010 to 2011, about 776,000 computers in more than 100 countries used Gnutella to share CSAM.[60] About 260,000 of those computers were located in the United States.[61] From those American computers, more than 5,000 CSAM images were shared more than 26,000 times per day.[62]

III. THE CURRENT STATE OF THE LAW

a. Laws Regulating CSAM on Social Media Platforms

The Electronic Communications Privacy Act of 1986 (ECPA)[63] protects the privacy of electronic, oral, and wire communications, including electronically stored data such as CSAM. More specifically, Title II of the ECPA, known as the Storage Communications Act (SCA),[64]

---

[57] Sextortion is the extortion of the minor by threatening to distribute their CSAM in exchange for more material, money, or other demands, which is like blackmail.

[58] Midwest Regional Children's Advocacy Center, *Implications of Social Media Use and Exposure to Pornography and Child Sexual Abuse Material (CSAM): The Role of the Medical Provider*, at 2, https://www.mrcac.org/wp-content/uploads/2023/07/Social-Media-Use-and-Exposure-to-Porn-CSAM.pdf. (citing Celeste Krewson, *Sexual Abuse Prevalent Against Teenagers in the United States*, CONTEMPORARY PEDIATRICS (Oct. 20, 2022), https://www.contemporarypediatrics.com/view/sexual-abuse-prevalent-against-teenagers-in-the-united-states).

[59] Thiel & DiResta, *supra* note 56 at 6–9.

[60] Emily D. Gottfried, Emily Knight Shier, & Abby L. Mulay, *Child Pornography and Online Sexual Solicitation*, 22 CURRENT PSYCHIATRY REPORTS (2020) (citing Janis Wolak, Marc Liberatore, & Brian Neil Levine, *Measuring a year of child pornography trafficking by U.S. computers on a peer-to-peer network*, 38 JOURNAL OF CHILD ABUSE & NEGLECT (2014), https://www.sciencedirect.com/science/article/abs/pii/S0145213413003232).

[61] *Id.*

[62] *Id.*

[63] Since 1986, the ECPA has been amended by the following: the 1994 Communications Assistance to Law Enforcement Act (CALEA), the 2001 USA PATRIOT Act, the 2006 USA PATRIOT reauthorization acts, the FISA Amendments Act of 2008, and others. *Electronic Communications Privacy Act of 1986 (ECPA)*, BUREAU OF JUSTICE ASSISTANCE, U.S. DEPARTMENT OF JUSTICE, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285.

[64] 18 U.S.C. §§ 2701–12.

maintains privacy safeguards for service providers' stored content and subscriber information. Generally speaking, electronic communication service companies cannot voluntarily disclose communications or subscriber/customer records that they facilitate.[65] However, there are some exceptions.[66] For example, these companies may voluntarily disclose communications to law enforcement if "the contents…were inadvertently obtained by the service provider…and appear to pertain to the commission of a crime,"[67] while customer records may be divulged "to any person other than a governmental entity."[68] However, both communications and customer records may be disclosed to NCMEC pursuant to 18 U.S.C. § 2258A[69] and as otherwise provided in other code sections such as 18 U.S.C. § 2703.[70]

Under the latter exception, 18 U.S.C. § 2703 outlines the legal procedures that law enforcement must follow in order to compel communications from these companies, including social media companies. Some of these procedures include obtaining search warrants, court orders, or user consent.[71] If the government follows the correct procedures, certain identifiable information is required to be disclosed to the government entity, including the user's name, address, identifying number or network address, and payment information. When this happens, the user does not know such information has been shared with the government.[72] In addition, upon receipt of request for such information, these providers have a duty to take any measure necessary to preserve these records and other evidence so that they can provide it in later proceedings.[73]

The other exception, 18 U.S.C. § 2258A, imposes a duty on these companies, including social media companies, to report violations of law related to CSAM and sex trafficking of minors.[74] This includes both apparent CSAM and imminent CSAM based on the facts or circumstances of the content.[75] The provider's report to NCMEC may include identifying information about the user, the user's history of content on the platform, the user's geographic location, visual depictions of the CSAM being reported, and any communications surrounding the CSAM.[76] After NCMEC receives such a report, they must share the report with the appropriate law enforcement agency.[77] The provider must then preserve the data or files reported for one year after the submission to NCMEC.[78]

Notably, these companies have no duty to monitor their platforms for criminal activity, including CSAM, or proactively ensure that these materials are not distributed on their platforms.

---

[65] 18 U.S.C. § 2702(a).
[66] 18 U.S.C. § 2702(b)–(c).
[67] 18 U.S.C. § 2702(b)(7).
[68] 18 U.S.C. § 2702(c)(6).
[69] 18 U.S.C. § 2702(b)(6), (c)(5).
[70] 18 U.S.C. § 2702(b)(2), (c)(1).
[71] 18 U.S.C. § 2703(c)(1).
[72] *See* 18 U.S.C. § 2703(c)(3).
[73] *See* 18 U.S.C. § 2703(f)(1).
[74] 18 U.S.C. § 2258A(a)(1).
[75] *See* 18 U.S.C. § 2258A(a)(2).
[76] *See* 18 U.S.C. § 2258A(b), (g)(3).
[77] 18 U.S.C. § 2258A(c).
[78] 18 U.S.C. § 2258A(h).

In fact, that lack of duty is explicitly stated in the law.[79] Social media companies are generally not required to share criminal activity taking place on their platforms with law enforcement, unless they are obligated by law to do so.

Nonetheless, the consequences for failure to report CSAM that companies have encountered can be costly. These companies may be fined between $600,000 to $1 million for a knowing and willful failure to report depending on the size of the company and the number of offenses.[80] Section 230 of the Communications Decency Act of 1996, however, "provides immunity to online platforms from civil liability based on third-party content and for the removal of content in certain circumstances."[81] The policy goal of this provision is to encourage these sites to removal illegal content like CSAM and foster an environment in which online media can thrive.[82] That being said, the protection that civil immunity provides may pose challenges in the enforcement of CSAM violations of these platforms. Most notably, immunity from liability disincentivizes platforms from taking a more aggressive stance against CSAM measures on their sites.

b. The Role of Government Agencies and Programs in Combatting CSAM

The production, distribution, and possession of CSAM are strictly criminalized on both the state and federal levels.[83] Social media can be used as a tool in law enforcement's arsenal in aiding their investigations into CSAM and other crimes.[84] On public social media sites, law enforcement can access profiles, content, and other information without authorization. They can also make posts of their own to track down suspects or make the public aware of certain initiatives.[85]

A number of federal and international government agencies and programs work to stop and prevent CSAM on social media and other online platforms, including the Internet Crimes Against Children (ICAC) Task Force program;[86] the Federal Bureau of Investigation's (FBI) Violent Crimes Against Children (VCAC) program;[87] the U.S. Department of Justice's Child Exploitation and Obscenity Section (CEOS);[88] the Homeland Security Investigations (HSI) branch

---

[79] Nothing in this section shall be construed to require a provider to— (1) monitor any user, subscriber, or customer of that provider; (2) monitor the content of any communication of any person described in paragraph (1); or (3) affirmatively search, screen, or scan for facts or circumstances described in sections (a) and (b). 18 U.S.C. § 2258A(f).

[80] 18 U.S.C. § 2258A(e).

[81] *Department Of Justice's Review Of Section 230 Of The Communications Decency Act Of 1996*, U.S. DEPARTMENT OF JUSTICE, https://www.justice.gov/archives/ag/department-justice-s-review-section-230- communications-decency-act-1996. *See* 47 U.S.C. § 230(c).

[82] *See* 47 U.S.C. § 230(b).

[83] *See* 18 U.S.C. §§ 1466A, 2251–2253.

[84] *See* Rachel Levinson-Waldman, *Principles for Social Media Use by Law Enforcement*, BRENNAN CENTER FOR JUSTICE (Feb. 7, 2024), https://www.brennancenter.org/our-work/research-reports/principles-social-media-use-law-enforcement.

[85] *Law Enforcement and Technology: Using Social Media*, CONGRESSIONAL RESEARCH SERVICE, (January 2022), https://sgp.fas.org/crs/misc/R47008.pdf.

[86] *Internet Crimes Against Children Task Force Program*, OFFICE OF JUVENILE JUSTICE AND DELINQUENCY PREVENTION, U.S. DEPARTMENT OF JUSTICE, https://ojjdp.ojp.gov/programs/internet-crimes-against-children-task-force-program.

[87] *Violent Crimes Against Children*, FEDERAL BUREAU OF INVESTIGATION, https://www.fbi.gov/investigate/violent-crime/vcac.

[88] *CEOS Mission*, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE, https://www.justice.gov/criminal/criminal-ceos/ceos-mission (last updated Aug. 11, 2023).

of the U.S. Immigration and Customs Enforcement (ICE);[89] NCMEC, the International Centre for Missing & Exploited Children (ICMEC)[90] and its U.S. Financial Coalition Against Child Sexual Exploitation (FCACSE);[91] and Interpol.[92] These agencies and programs work to spread awareness about CSAM and child exploitation, investigate possible crimes on these platforms, and work with law enforcement to bring offenders to justice.

However, these bodies face many challenges to regulation. While some offenders use rudimentary routes to access and save CSAM online, others utilize sophisticated technology and encryption when committing their crimes.[93] Such advanced technology often present barriers to law enforcement, including digital forensic analysis that cannot be completed in a timely manner.[94] In addition, such complex technology also makes it harder for law enforcement to catch and trace CSAM in the first place. Social media companies also often have concerns surrounding privacy, specifically regarding sharing data and user information with law enforcement and government agencies. This can result in "delays in obtaining identifying information from IPSs [internet service providers] regarding their customers suspected of distributing child pornography."[95] However, perhaps the most disturbing challenge of all is sorting through the massive volume of CSAM on these sites.[96]

IV. WHAT SOCIAL MEDIA COMPANIES CURRENTLY DO

The U.S. Government does not require social media companies to actively sort through CSAM on their sites. If they do become aware, then these companies are required by law to report it to NCMEC.[97] Some social media companies independently take extra measures to stop CSAM on their sites.[98] For example, many social media sites offer reporting mechanisms for CSAM and other content that violates the terms of service.[99] Additionally, TikTok has established a "zero-tolerance approach" to CSAM and encourages the use of age controls and restrictions on the app.[100] Google supports some of the proposed legislation for stronger protections, and works with

---

[89] *Child Exploitation*, Homeland Sec. Investigations, U.S. DEP'T. OF HOMELAND SEC., https://www.dhs.gov/hsi/investigate/child-exploitation (last updated Aug. 7, 2024).

[90] *Our Mission: About ICMEC*, INTL'L CTR. FOR MISSING & EXPLOITED CHILD., https://www.icmec.org/about/.

[91] *U.S. Financial Coalition Against Child Sexual Exploitation*, INT'L CTR. FOR MISSING & EXPLOITED CHILD., https://www.icmec.org/fcacse/.

[92] *International Child Sexual Exploitation Database*, INTERPOL, https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database.

[93] *Federal Child Pornography Offenses,* U.S. SENTENCING COMM'N, 71–72*,* https://www.ussc.gov/sites/default/files/pdf/news/congressional-testimony-and-reports/sex-offense-topics/201212-federal-child-pornography-offenses/Full_Report_to_Congress.pdf.

[94] *Id.* at 72.

[95] *Id.*

[96] *Id.*

[97] 18 U.S.C. § 2258A(a) (2022).

[98] *See* Coen Teunissen & Sarah Napier, *Child Sexual Abuse Material and End-to-End Encryption on Social Media Platforms: An Overview*, AUSTL. GOV'T: AUSTL. INST. OF CRIMINOLOGY, at 7–9 (July 2022), https://www.aic.gov.au/sites/default/files/2022-07/ti653_csam_and_end-to-end_encryption_on_social_media_platforms-v2.pdf.

[99] Neeraj Soni, *Navigating the Social Media Complaint Reporting Mechanism*, CYBERPEACE (Sept. 26, 2023), https://www.cyberpeace.org/resources/blogs/navigating-the-social-media-complaint-reporting-mechanism.

[100] *Age Appropriate Experiences*, TIKTOK, https://www.tiktok.com/legal/page/global/age-appropriate-experiences/en.

NCMEC and child experts to stop CSAM on their platforms.[101] Google also publishes a transparency report that shows how many CyberTipline reports they have made, how many accounts have been identified as CSAM offenders, how many hashes they have added to the NCMEC database, and more.[102] Facebook has voiced commitments to not only detect, report, and remove CSAM, but also to prevent it altogether.[103] In 2021, Facebook also introduced a feature that prevents users from searching for CSAM on the site.[104] As a result of these efforts, millions of files have been removed, and millions of accounts have been identified.

However, other companies offer virtually no protections. Telegram allows CSAM distribution through private channels. Discord has almost no safeguards to prevent children from meeting predators online.[105] A vast majority of sextortion occurs on sites like Wizz,[106] Instagram, TikTok, and Snapchat, despite any protections they may have.[107] In 2022, the U.S. Senate Judiciary Committee Chair Dick Durbin confronted Elon Musk about his failed promises to rid his platform X of child sexual exploitation,[108] to which Musk did not respond.

In fact, many of the world's largest social media companies are simply not doing enough. On January 31, 2024, the Senate Judiciary Committee held a full committee hearing featuring CEOs from a number of the most popular social media companies: Mark Zuckerberg from Meta, Lina Yaccarino from X, Shou Xi Chew from TikTok, Evan Spiegel from Snapchat, and Jason Citron from Discord. The hearing featured testimony from all of these CEOs regarding the prevalence of CSAM and child exploitation online, as well as what they can do to prevent it.[109] The hearing called for transparency and accountability from the social media companies, as well as the need for collaboration between the government and these platforms.[110] However, the Committee made one major finding that summarizes the meeting: "social media companies have

---

[101] Susan Jasper, *An Update on Our Child Safety Efforts and Commitments*, GOOGLE: THE KEYWORD (Apr. 23, 2024), https://blog.google/technology/safety-security/an-update-on-our-child-safety-efforts-and-commitments/.

[102] *Google's Efforts to Combat Online Child Sexual Abuse Material*, GOOGLE TRANSPARENCY REP., https://transparencyreport.google.com/child-sexual-abuse-material/reporting?hl=en.

[103] John Buckley, Malia Andrus & Chris Williams, *Understanding the Intentions of Child Sexual Abuse Material (CSAM) Sharers*, META (Feb. 23, 2021), https://research.facebook.com/blog/2021/2/understanding-the-intentions-of-child-sexual-abuse-material-csam-sharers/.

[104] Pounder & Turek, *supra* note 53.

[105] Ahsan Habib, *CSAM: The Role of Social Media and Jurisdictions*, ACAMS TODAY (Apr. 23, 2024), https://www.acamstoday.org/csam-the-role-of-social-media-and-jurisdictions/.

[106] *See Is the Wizz App Dangerous for Kids? A Safety Guide to 'Teen Tinder'*, QUSTODIO BY QORIA (Feb. 15, 2024), https://www.qustodio.com/en/blog/is-wizz-app-dangerous/.

[107] Ahsan Habib, *CSAM: The Role of Social Media and Jurisdictions*, ACAMS TODAY (Apr. 23, 2024), https://www.acamstoday.org/csam-the-role-of-social-media-and-jurisdictions/ (citing Kevin Poireault, *Nigerian 'Yahoo Boys' Behind Social Media Sextortion Surge in the US*, INFOSECURITY MAG. (Jan. 29, 2024), https://www.infosecurity-magazine.com/news/nigerian-yahoo-boys-social-media/).

[108] *See* Alix Fraser et al., *Protecting Children Online — Questions for Five Big Tech CEOs*, TECH POL'Y PRESS (Jan. 26, 2024), https://www.techpolicy.press/protecting-children-online-questions-for-five-big-tech-ceos/.

[109] *Protecting Children Online: Hearing Before the S. Comm. on the Judiciary*, 118th Cong. (2024), https://www.judiciary.senate.gov/protecting-children-online.

[110] *Key Takeaways from the Online Child Sexual Exploitation Hearing with Social Media CEOs*, SAFER (Feb. 2, 2024), https://safer.io/resources/key-takeaways-from-the-online-child-sexual-exploitation-hearing-with-social- media-ceos/; *see also* Barbara Ortutay & Haleluya Hadero, *Meta, TikTok and Other Social Media CEOs Testify in Heated Hearing on Child Exploitation*, ASSOCIATED PRESS, https://apnews.com/article/meta-tiktok-snap-discord- zuckerberg-testify-senate-00754a6bea92aaad62585ed55f219932 (Jan. 31, 2024, 8:26 PM).

failed to police themselves at our kids' expense, and now Congress must act."[111]

Part of this shortcoming comes from the government explicitly not imposing a duty on social media companies to act.[112] Instead, they only have to report CSAM to the CyberTipline if they become aware of its existence on their platform[113] or else they can be fined up to $1 million.[114] However, this potential fine may not be sizeable in the eyes of billion-dollar social media companies. In addition, a fine of $1 million may be cheaper for a company than taking further steps to prevent CSAM. Monitoring requires human moderators,[115] AI programs, the implementation of programs, constant updates, expanded data storage, and increased data privacy, which could cost millions, if not billions, of dollars to fund.[116]

Another incentive for social media companies to further implement CSAM detection and removal systems may be to avoid a bad reputation.[117] Parents do not want their children on a platform that does not offer protections to ensure age-appropriate content. The vast majority of users do not want the "wild west" of platforms where they may be exposed to criminal content. Additionally, many people, in general, do not want to support a company they consider immoral.[118] In today's age, when news is easily accessible at our fingertips, a company's reputation can be destroyed in a matter of seconds. Therefore, social media companies only do just enough to prevent CSAM to avoid hitting the headlines. As much as these companies do not want a reputation for facilitating CSAM, they want to avoid a reputation for intruding on users even more.[119] In this political climate, many social media companies are staunch advocates for the freedoms of speech and expression, as some companies believe imposing greater restrictions would violate such rights.[120]

---

[111] Joao-Pierre S. Ruth, *Senate Hearing and Big Tech's Social Media* Responsibility, INFO. WEEK (Feb. 5, 2024), https://www.informationweek.com/data-management/senate-hearing-and-big-tech-s-social-media-responsibility.
[112] 18 U.S.C. § 2258A(f).
[113] 18 U.S.C. § 2258A(a).
[114] 18 U.S.C. § 2258A(e).
[115] *See* David Thiel & Renée DiResta, *Child Safety on Federated Social Media,* STAN. INTERNET OBSERVATORY, 10 (2023), https://stacks.stanford.edu/file/druid:vb515nd6874/20230724-fediverse-csam-report.pdf.
[116] *AI Pricing: How Much Does Artificial Intelligence Cost?,* WEBFX, https://www.webfx.com/martech/pricing/ai/.www.webfx.com/martech/pricing/ai/ (last visited Dec. 20, 2024).
[117] Rhiannon Williams, *The US Now Hosts More Child Sexual Abuse Material Online Than Any Other Country*, MIT TECH. REV. (Apr. 26, 2022), https://www.technologyreview.com/2022/04/26/1051282/the-us-now-hosts-more-child-sexual-abuse-material-online-than-any-other-country/.
[118] *See* Kat Tenbarge & Kevin Collier, *X Sees Largest User Exodus Since Elon Musk Takeover*, NBC NEWS (Nov. 13, 2024, 4:40 PM), https://www.nbcnews.com/tech/tech-news/x-sees-largest-user-exodus-musk-takeover-rcna179793.
[119] Michael Salter, Delanie Woodlock, & Tim Wong, *The Sexual Politics of Technology Industry Responses to Online Child Sexual Exploitation During COVID-19: "This Pernicious Elitism"*, J. OF CHILD ABUSE & NEGLECT at 2–3 (Nov. 13, 2023), https://www.sciencedirect.com/science/article/pii/S0145213423005471#bb2005 (citing Michael Salter, *Online Child Sexual Exploitation in the News*, *in* THE ROUTLEDGE COMPANION TO GENDER, MEDIA, AND VIOLENCE 401-11 (Karen Boyle & Susan Berridge, eds., 2023), https://www.taylorfrancis.com/chapters/edit/10.4324/9781003200871-44/online-child-sexual-exploitation-news-michael-salter).
[120] Michael Salter, Delanie Woodlock, & Tim Wong, *The Sexual Politics of Technology Industry Responses to Online Child Sexual Exploitation During COVID-19: "This Pernicious Elitism"*, J. OF CHILD ABUSE & NEGLECT at 3 (Nov. 13, 2023), https://www.sciencedirect.com/science/article/pii/S0145213423005471#bb2005 (citing Ellie Hanson, *'Losing Track of Morality': Understanding Online Forces and Dynamics Conducive to Child Sexual Exploitation, in*

V. WHAT SHOULD BE DONE

Given social media companies' generally ineffective response to the CSAM problem, the government take the reins. The government should pass proposed legislation with stricter guidelines, impose a duty on social media companies to monitor their sites for CSAM, and require these online service providers to implement AI programs to remove these materials.

a. Proposed Legislation

Proposed legislation may offer support in the country's fight against CSAM and child sexual exploitation, and many national groups advocate for the passage of such bills. The Rape, Abuse & Incest National Network (RAINN), the largest anti-sexual violence organization in the U.S.,[121] has pushed for Congress to pass the Child Rescue Act and the Project Safe Childhood Modernization Act.[122] Introduced in April 2024, the Child Rescue Act would "direct the Attorney General to convene a national working group to study proactive strategies and needed resources for the identification and rescue of children from sexual exploitation and abuse."[123] Introduced a year earlier, the Project Safe Childhood Modernization Act "modifies and reauthorizes through FY2028 the Project Safe Childhood Program within the Department of Justice," which "coordinates child sexual exploitation investigations and prosecutions across federal, state, and local law enforcement; provides training to law enforcement on best practices; and supports public education programs."[124] Additionally, the National Children's Alliance (NCA), a national professional membership organization which has served almost two million through their Children Advocacy Centers,[125] supported the passage of U.S. National Blueprint to End Sexual Violence Against Children and Adolescents.[126] Focused on prevention, healing, and justice, the Blueprint calls for the government to take a series of actionable steps against CSAM and child exploitation.[127] These proposed laws are a solid foundation upon which the other two parts of my proposals build.

Some government entities have also added to the conversation. The Department of Justice (DOJ) has proposed amendments to Section 230 of the Communications Decency Act of 1996.[128] Instead of full civil immunity, DOJ suggests carve-outs for companies acting in bad faith and for child abuse content.[129] NCMEC also advocates for the passage of the Strengthening Transparency

---

CHILD SEXUAL EXPLOITATION: WHY THEORY MATTERS, 87–116 (Jenny Pearce, ed., 2019), https://bristoluniversitypressdigital.com/edcollchap/book/9781447351429/ch005.xml).

[121] *Mission Statement*, RAINN, https://rainn.org/mission-statement, (last visited Dec. 20, 2024).

[122] *What Is Child Sexual Abuse Material (CSAM)*, RAINN (Aug. 25, 2022), https://rainn.org/news/what-child-sexual-abuse-material-csam.

[123] Child Rescue Act, H.R. 8183, 118th Cong. (2024).

[124] Project Safe Childhood Act, H.R. 2661, 118th Cong. (2023).

[125] *About: Our Story*, NAT'L CHILD.'S ALL., https://www.nationalchildrensalliance.org/our-story/.

[126] *Advocacy: Our Positions*, NAT'L CHILD.'S ALL., https://www.nationalchildrensalliance.org/supported-legislation/.

[127] *Introducing the U.S. National Blueprint*, KEEP KIDS SAFE, https://www.keepkidssafe.us/the-blueprint#read-the-blueprint-desktop.

[128] *DEPARTMENT OF JUSTICE'S REVIEW OF SECTION 230 OF THE COMMUNICATIONS DECENCY ACT OF 1996*, U.S. DEP'T OF JUST., https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996.

[129] *Section 230 — Nurturing Innovation or Fostering Unaccountability?: Key Takeaways and Recommendations*, U.S. DEP'T OF JUST. (June 2020), https://www.justice.gov/ag/media/1072971/dl?inline=.

and Obligation to Protect Children Suffering from Abuse and Mistreatment Act of 2023 (STOP CSAM). The Act is a comprehensive bill that, among other things, "improves reporting of [CSAM] to NCMEC's CyberTipline; creates transparency requirements for online platforms; increases accountability for online platforms knowingly hosting, storing, promoting, or facilitating the distribution of CSAM; and . . . creat[es] a Report and Remove program to formalize requests to online platforms to remove CSAM."[130] However, even bipartisan legislation such as the above act[131] has been criticized over freedom of expression and privacy rights concerns.[132]

b. Duty to Monitor

The United States should impose a duty on social media companies and other electronic communications providers to actively monitor their sites for CSAM and evidence of other criminal activity. Other parts of the world already impose such a duty. For example, the European Union's Digital Services Act (DSA) imposes a duty on social media companies and other similar platforms to put measures in place to combat illegal content online. These measures include providing users with easy ways to flag suspicious content and working with trusted flaggers to evaluate such reports.[133] Article 24(b) of the DSA further strengthened protections against user-generated CSAM.[134] Similarly, in the United Kingdom, the Online Safety Act (OSA) imposes a duty on companies like social media sites to monitor and search their platforms for illegal content and CSAM. On January 31, 2024, criminal offenses went into effect for a number of other violations related to CSAM as well.[135]

However, the effectiveness of the DSA and the OSA are unknown. The DSA was issued in December 2020[136] and went "into full effect" in February 2024.[137] The OSA is also fairly new,

---

[130] *The STOP CSAM ACT*, NAT'L CTR. FOR MISSING & EXPLOITED CHILD., https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-support-stop-csam-act.pdf; *see* STOP CSAM Act of 2023, S. 1199, 118th Cong. (2023).

[131] *Rep. Barry Moore Introduces Bipartisan Legislation to Protect Children Online*, BARRY MOORE (Apr. 12, 2024), https://barrymoore.house.gov/media/press-releases/rep-barry-moore-introduces-bipartisan-legislation-protect-children-online.

[132] Emma Llansó, *The STOP CSAM Act Threatens Free Expression and Privacy Rights of Children and Adults*, CTR. FOR DEMOCRACY & TECH. (May 2, 2023), https://cdt.org/insights/the-stop-csam-act- threatens-free-expression-and-privacy-rights-of-children-and-adults/.

[133] *The Digital Services Act*, EUR. COMM'N, https://commission.europa.eu/strategy-and-policy/priorities- 2019-2024/europe-fit-digital-age/digital-services-act_en. See *The Digital Services Act: Practical Implications for Online Services and Platforms*, LATHAM & WATKINS LLP (Mar. 2023), https://www.lw.com/admin/upload/SiteAttachments/Digital-Services-Act-Practical-Implications-for-Online- Services-and-Platforms.pdf.

[134] Lorna Woods & Clare McGlynn, *Pornography Platforms, the EU Digital Services Act and Image-Based Sexual Abuse*, THE LONDON SCH. OF ECON. & POL. SCI. (Jan. 26, 2022), https://blogs.lse.ac.uk/medialse/2022/01/26/pornography-platforms-the-eu-digital-services-act-and-image-based- sexual-abuse/.

[135] *Online Safety Act: Explainer*, GOV.UK: DEP'T FOR SCI., INNOVATION, & TECH. (May 8, 2024), https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer.

[136] Aina Turillazzi, Mariarosaria Taddeo, Luciano Floridi, & Federico Casolari, *The Digital Services Act: An Analysis of its Ethical, Legal, and Social Implications*, 15 L., INNOVATION & TECH. 83, 83 (2023). www.tandfonline.com/doi/epdf/10.1080/17579961.2023.2184136?needAccess=true.

[137] Gabby Miller, *The Digital Services Act is Fully in Effect, But Many Questions Remain*, TECH POL'Y PRESS, (Feb. 20, 2024), https://www.techpolicy.press/the-digital-services-act-in-full-effect-questions-remain/.

as it was enacted in October 2023.[138] That being said it is expected that these laws will result in increased CSAM detection and removal. If social media companies are statutorily required to constantly look for CSAM, they must take actionable steps to seek it out instead of passively waiting for someone to come across such material and report it to them. Not only will actively searching be more effective to finding more CSAM, but it will also be quicker than the current process. By eliminating the reliance on a middleman (the user) to find and report these materials, these companies can find these files themselves and remove them immediately.

The U.S. government should impose this duty to monitor for the above reasons. However, there may be constitutional obstacles to this proposal. The Fourth Amendment protects citizens against "unreasonable searches and seizures" by the government.[139] Typically, law enforcement must obtain a warrant showing probable cause in order to perform a search. One exception to this requirement is if there are exigent circumstances. This means that warrantless searches are valid if a reasonable person would believe that entry is necessary to provide emergency assistance; catch a fleeing suspect;[140] prevent physical harm; destruction of evidence; escape; or "some other consequence improperly frustrating legitimate law enforcement efforts."[141] Notably, the Fourth Amendment only applies to government action,[142] while this proposal concerns searches conducted by social media companies. However, warrantless searches are unconstitutional when performed by private parties "if the private party act[s] as an instrument or agent of the Government."[143] Thus, these CSAM searches of users by social media companies may constitute Fourth Amendment violations.

That being said, this proposal does not violate the Fourth Amendment. Under the private search doctrine, private actors can give the government evidence of criminal activity they find in the course of a warrantless search, and the government may use that evidence in their prosecution of that individual.[144] In other words, "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."[145] If social media companies find CSAM on their platforms, the government can use those materials as evidence. Furthermore, social media companies are not acting as government instruments or agents. The company is a completely separate entity, which may be regulated by the government. Although social media companies would be statutorily required to search for CSAM, it is only an initial indication to law enforcement. A secondary search conducted by law enforcement of that potential offender, however, would require a warrant.[146]

Additionally, in some situations, CSAM found by social media companies may constitute exigent circumstances. If there is evidence of ongoing child sexual exploitation, the circumstances

---

[138] Peter Coe, *Tackling Online False Information in the United Kingdom: The Online Safety Act 2023 and Its Disconnection from Free Speech Law and Theory*, 15 J. OF MEDIA L. 213, 214 (2023). www.tandfonline.com/doi/epdf/10.1080/17577632.2024.2316360?needAccess=true.
[139] U.S. CONST. amend. 4.
[140] *See Missouri v. McNeely*, 569 U.S. 141 (2013).
[141] *United States v. McConney*, 728 F.2d 1195 (9th Cir. 1984).
[142] *See United States v. Jacobsen*, 466 U.S. 109 (1984).
[143] *Skinner v. Railway Labor Executives' Assn.*, 489 U.S. 602 (1989).
[144] *See McNeely*, *supra* note 140.
[145] *United States v. Miller*, 425 U.S. 435, 443 (1976).
[146] *See United States v. Carpenter,* 585 U.S. 296 (2018).

may demonstrate a need for immediate intervention. Lastly, individuals and entities have a reasonable expectation of privacy,[147] however, a warrant is not required to obtain information when parties knowingly expose that information to a third party.[148] In this situation, social media companies facilitate user-generated content on their platforms. As such, users share content, such as CSAM, with social media companies, which eliminates the need for a warrant.

c. AI Programs

By far, the biggest obstacle in the fight to eradicate CSAM from the internet, specifically on social media, is the sheer volume of these materials. It seems as though there is a never-ending stream of this abuse online, even as law enforcement tries their best to detect and remove these materials. Simply put, there is too much CSAM online for humans to sift through.

Luckily, technological advances may offer a solution: artificial intelligence (AI). Although definitions vary, AI is generally "an interdisciplinary branch of computer science that deals with models and data processing systems for the performance, emulation, or recreation of functions that earlier have been associated with human intelligence, such as reasoning, learning, and self-improvement."[149] At its core, AI imitates human cognition by learning through experiences via algorithms and pattern recognition.[150] There are also different types of AI: reactive, predictive, and generative. Reactive AI responds to certain inputs, such as Siri responding to prompts on Apple devices. Predictive AI uses data analysis to make predictions, such as personalized suggested shows on Netflix. Generative AI, like ChatGPT, creates original content.[151] In the context of CSAM detection and removal, the focus is on reactive AI.[152]

There are a number of advantages to using AI in the pursuit of CSAM eradication from social media. AI is adaptable, given that it is constantly learning from inputted information and can be catered to whatever goal the developer aims to achieve. It generally computes with less errors due to automation, as opposed to humans who constantly make mistakes. Thus, AI enhances efficiency for users and can be more productive in less time. Additionally, it is available twenty-four hours a day, seven days a week, so AI programs can run without needing a break like humans would. These programs would also make searching for CSAM easier, as the process would be

---

[147] *See Katz v. United States,* 389 U.S. 347 (1967).

[148] *See Smith v. Maryland*, 442 U.S. 735 (1979). *See also United States v. Miller*, 425 U.S. 435 (1976).

[149] Emile Loza de Siles, *AI, on the Law of the Elephant: Toward Understanding Artificial Intelligence*, 69 BUFFALO LAW REVIEW 1418 (2021), https://digitalcommons.law.buffalo.edu/cgi/viewcontent.cgi?article=4928&context=buffalolawreview. (citing *Artificial Intelligence*, DICTIONARY.COM, https://www.dictionary.com/browse/artificial-intelligence; High-Level Expert Group on A.I., Eur. Comm'n, *A Definition Of AI: Main Capabilities and Scientific Disciplines* 7 (Dec. 18, 2018)).

[150] *What is (AI) Artificial Intelligence?,* UNIVERSITY OF ILLINOIS CHICAGO, (May 7, 2024), https://meng.uic.edu/news-stories/ai-artificial-intelligence-what-is-the-definition-of-ai-and-how-does-ai-work/.

[151] *Pros and Cons of AI in the Future of Education*, NATIONAL MATH + SCIENCE INITIATIVE, (Aug. 16, 2024), https://www.nms.org/Resources/Newsroom/Blog/2024/August-2024/Pros-and-Cons-of-AI-in-the-Future-of-Education.aspx.

[152] Especially in the last couple of years, discussion and legislation regarding generative AI CSAM has become more prominent. AI models are being trained to create fake materials depicting child sexual abuse. This paper is not focused on that very broad topic, but it is related to the contents of this paper. *Generative AI CSAM is CSAM*, NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN, (March 11, 2024), https://www.missingkids.org/blog/2024/generative-ai-csam-is-csam.

completely automated, with the exception of occasional human review. AI programs can also be integrated into systems that are already in place, so companies can easily implement such programs.[153]

Steps are already being taken by the government to use AI to detect and remove CSAM. On October 30, 2023, President Biden signed an Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence.[154] In the Order, he charged several government agencies, including the National Institute of Standards and Technology (NIST), with establishing standards for the use of AI systems within the government. CSAM was specifically included as a target of such programs.[155]

One example of an AI program used for this purpose is Microsoft's PhotoDNA. Developed in 2009 in partnership with Dartmouth College, PhotoDNA is a program that helps to identify and remove CSAM from the internet. When the program detects an image, it creates a unique digital signature (called a "hash") for the image, which is like a fingerprint for the image. Then, the image's hash is compared to hashes contained in a NCMEC database composed of the illegal images that have been previously identified.[156] When the image's hash matches that of a known illegal image, it can be detected and removed without human intervention.

Since its inception, PhotoDNA has aided, detected, disrupted, and reported millions of these files from around the world.[157] It is highly effective and very accurate, with an almost 0% rate of false positive matches and a less than 2% rate of false negatives.[158] In 2009, Microsoft donated the program to NCMEC to enhance their systems in place in the fight against CSAM and enable online service providers, like social media companies, to better equip them in their fight as well.[159] In 2015, Microsoft expanded the impact of PhotoDNA by making it available on Microsoft Azure,[160] allowing even more companies to detect and remove CSAM from their platforms.[161] Today, PhotoDNA is available for free to qualified businesses,[162] such as developers, non-profit

---

[153] Nikita Duggal, *Incredible Advantages of AI: Notable 23 Benefits of AI*, SIMPLILEARN, (Oct. 22, 2024), https://www.simplilearn.com/advantages-and-disadvantages-of-artificial-intelligence-article.

[154] Exec. Order No. 14110, 88 Fed. Reg. 75191 (Oct. 30, 2023).

[155] *Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, https://www.nist.gov/artificial-intelligence/executive-order-safe-secure-and-trustworthy- artificial-intelligence.

[156] Ilana Berger & Time Torres, *Detecting Novel CSAM – Why Image Hash Matching Isn't Enough Anymore*, ACTIVEFENCE, (July 12, 2024), https://www.activefence.com/blog/detecting-csam-hash-matching/.

[157] *PhotoDNA*, MICROSOFT, https://www.microsoft.com/en-us/photodna?oneroute=true (last visited Feb. 15, 2025).

[158] Martin Steinebach, *An Analysis of PhotoDNA*, ASSOCIATION OF COMPUTING MACHINERY (August 2023), https://dl.acm.org/doi/10.1145/3600160.3605048.

[159] *Microsoft and National Center for Missing & Exploited Children Push for Action to Fight Child Pornography,* MICROSOFT (Dec. 15, 2009), https://news.microsoft.com/2009/12/15/microsoft-and-national-center-for-missing-exploited-children-push-for-action-to-fight-child-pornography/

[160] Microsoft Azure is a part of the Microsoft suite used by businesses as an infrastructure tool. It is "a public cloud computing platform…that can be used for services such as analytics, virtual computing, storage, networking, and much more. It can be used to replace or supplement [their] on-premise servers." Logan McCoy, *Microsoft Azure Explained: What It Is and Why It Matters*, CCB TECHNOLOGY, https://ccbtechnology.com/what-microsoft-azure-is-and-why-it-matters/ (last visited Feb. 15, 2025).

[161] *PhotoDNA*, *supra* note 154.

[162] "Qualified businesses" are vetted by a third-party service. However, the requirements for being considered "qualified" are unclear. Nevertheless, the businesses and online service providers using PhotoDNA must host user-

organizations, and technology companies. It is also now free to law enforcement, and is predominantly used by their forensic tool developers.[163]

Other programs go even further. Thorn, a non-profit organization that works to prevent child sexual abuse,[164] has an AI program called Safer Predict.[165] In 2019, Thorn launched Safer, a hashing AI program that worked essentially the same as PhotoDNA. Safer has proven to be successful, given that it has matched more than three million CSAM materials since its launch.[166] In 2024, they expanded the program by introducing Safer Predict, which detects new and unreported CSAM materials, instead of relying on database hash matches. Not only can Safer Predict identify new content, but it can also identify text, conversations about sextortion, self-generated CSAM, and potential abuse that may occur offline. Safer Predict has also been a success; it has already labeled 2 million files as potential CSAM.[167]

Nevertheless, there are a number of issues with AI programs: inputted data sets may be incomplete, algorithms may be biased, it takes time to develop more sophisticated technology, and, most notably, AI systems can be very expensive to create and implement.[168] Even if there are systems already in place into which AI can integrate, the price tag is still relatively high. Another issue with AI is that it is limited in its functions. Because AI programs learn from patterns and inputted data, the program may only be as good as the information it has analyzed. In addition, "AI systems cannot…match higher-order human abilities, such as abstract reasoning, concept comprehension, flexible understanding, [and] general problem-solving skills…. Instead, today's AI systems excel in narrow, limited settings…often where there are clear right or wrong answers where there are discernible underlying patterns and structures."[169] Essentially, as it currently stands, it is impossible for AI to completely take the place of humans in this space. Human moderators are still needed to review decisions made by the AI programs and work with law enforcement in the course of an investigation.

One particular problem with Microsoft PhotoDNA is the incomplete database to compare its detected images to illegal ones. The program works by comparing the hashes of the images it

---

generated content. *PhotoDNA Cloud Service: Organizations, Businesses & Non-Profits*, MICROSOFT, https://www.microsoft.com/en-us/photodna/CloudService?oneroute=true (last visited Feb. 15, 2025). https://www.microsoft.com/en-us/photodna/FAQ?oneroute=true (last visited Feb. 15, 2025).

[163] *PhotoDNA*, MICROSOFT, https://www.microsoft.com/en-us/photodna?oneroute=true.

[164] *Who We Are*, THORN, https://www.thorn.org/about/ (last visited Feb. 15, 2025); *PhotoDNA, supra* note 154.

[165] *Introducing Safer Predict: Using the Power of AI to Detect Child Sexual Abuse and Exploitation Online*, THORN, (July 19, 2024), https://www.thorn.org/blog/introducing-safer-predict-using-the-power-of-ai-to-detect-child-sexual-abuse-and-exploitation-online.

[166] *Id*. *See also Safeguard Your Brand with Comprehensive CSAM Detection,* SAFER BUILT BY THORN, https://safer.io/.

[167] *Who We Are*, *supra* note 161.

[168] *See* Antonio Pontón-Núñez, *Addressing the Risks and Harms of Artificial Intelligence by Leveraging Capital*, NONPROFIT QUARTERLY, (Apr. 8, 2024), https://nonprofitquarterly.org/addressing-the-risks-and-harms-of-artificial-intelligence-by-leveraging-capital/?gad_source=1&gclid=CjwKCAiApY-7BhBjEiwAQMrrEd0BJdAtr7w52Cbl07znN9XBMj6Acn978gDQdZM6XZ5SftWVGJ8rfxoC4HoQAvD_BwE.

[169] Harry Surden, *Artificial Intelligence and Law: An Overview*, 35 GEORGIA STATE UNIVERSITY LAW REVIEW 1309 (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3411869 (citing Jack Krupansky, *Untangling the Definitions of Artificial Intelligence, Machine Intelligence, and Machine Learning*, MEDIUM (June 13, 2017), https://medium.com/@jackkrupansky/untangling-thedefinitions-of-artificial-intelligence-machine-intelligence-and-machine-learning-7244882f04c7; John Rennie, *How IBM's Watson Computer Excels at Jeopardy!,* PLOS BLOGS (Feb. 14, 2011), https://www.cs.cornell.edu/courses/cs6700/2013sp/readings/01-a-Watson-Short.pdf).

detects to hashes in a database of hashes of known illegal images. However, there are many CSAM images that are not in the database, and more images are being created and uploaded every day. If an image is not in the database, PhotoDNA does not know to report it as CSAM. Simply put, hash matching is not enough. These programs need to account not only for known CSAM images but also for videos, text discussions, and newly generated content.[170] Safer Predict is, therefore, a better solution.

As Congress has previously expressed, social media companies have not done enough on their own to stop CSAM on their platforms. Congress has called on them, individually and collectively, to take actionable steps toward this goal.[171] I agree that social media companies should rise to that challenge on their own. However, I am not optimistic that they will actually do so. As history has shown, these companies will not implement measures to effectively act for a public concern as harmful and widespread as CSAM. Therefore, the government should step in via legislation to require that social media companies implement AI programs, like Safer Predict, onto their platforms so that CSAM can be detected and removed quicker and more effectively that the measures currently in place. There would have to be minimum requirements for these programs based on their effectiveness, accuracy, and data privacy. One obstacle to this proposal may be the cost of implementing these programs to satisfy compliance. However, the government could partially subsidize such an undertaking; the government could incentivize these companies to implement AI; or, depending on their size and net worth or market capitalization, these companies may be left to their own devices to fund the implementation.

VI. CONCLUSION

In summary, there is no easy solution to the problem of CSAM on social media. The government seems to point their finger at social media companies, while social media companies seem to do the bare minimum as required by the government. Because of this stand-still, I suggest that the government implement proposed legislation, impose a duty on these companies to monitor their platforms, and require social media companies to implement robust AI programs, like Safer Predict, to detect potential child sexual exploitation.

Thankfully, it is not just the government and social media companies who can work to solve these problems. There are a number of things the average person can do to stop the production, distribution, and possession of CSAM. Users can report suspicious content on their respective social media platforms and to NCMEC's Cyber Tipline. Parents can put privacy settings on their children's social media accounts and educate them about online safety practices. Law enforcement and prosecutorial agencies can educate the public about CSAM and child sexual exploitation, spread awareness, and support survivors.[172]

While the road to the elimination of CSAM may be a long one, it is a goal worth fighting

---

[170] Steinebach, *supra* note 155; *see also* Ilana Berger & Time Torres, *Detecting Novel CSAM – Why Image Hash Matching Isn't Enough Anymore*, ACTIVEFENCE, (July 12, 2024), https://www.activefence.com/blog/detecting-csam-hash-matching/.

[171] *Protecting Children Online*, U.S. SENATE COMMITTEE ON THE JUDICIARY, https://www.judiciary.senate.gov/protecting-children-online.

[172] *How to Prevent Child Sexual Abuse Material (CSAM)*, RAINN (July 12, 2023), https://rainn.org/news/how-prevent-child-sexual-abuse-material-csam.

toward in whatever way possible. If CSAM is Goliath, we must come together to muster the strength of David. I am optimistic about that future, one that hopefully comes as soon as possible.