THE GOVERNMENT IS IN YOUR DIRECT MESSAGES: DOES NEW LEGISLATION ALLOW TECH COMPANIES TO SEARCH YOUR ONLINE COMMUNICATIONS?

Maura Arnold*

I. Introduction

In 2019, technology (“tech”) companies reported 45 million online photos and videos of sexual abuse in the past year.1 These images and videos include children as young as three or four years old being sexually abused and even tortured.2 While child sexual abuse

*J.D. Candidate, Suffolk University Law School, 2022; B.A. English and Italian Studies, College of the Holy Cross, 2017. Maura can be reached at maura.arnold@gmail.com.

1 See Michael H. Keller & Gabriel J.X. Dance, The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong?, THE N.Y. TIMES (Sept. 29, 2019), archived at https://perma.cc/5MV5-VVJ6 (stating that “[t]echnology companies reported a record 45 million online photos and videos of the abuse last year.”). See also Joseph Jerome, Reconsidering the EARN IT Act, PROTEGO PRESS (Jan. 31, 2021), archived at https://perma.cc/3A6F-JKGJ (explaining how research surveys and newspapers have come to suggest that child sexual abuse material and crimes are steadily increasing); Abigail Slater, EARN IT Act Calls Internet Content Moderation Into Question, THE REGUL. REV. (Mar. 30, 2020), archived at https://perma.cc/7TRA-S2J9 (noting that in 2019, reports to the National Center for Missing and Exploited Children’s CyberTipline included 69.1 million forms of child sexual exploitation).

2 See Keller & Dance, supra note 1 (stating that images online include “[c]hildren, some just 3 or 4 years old, being sexually abused and in some cases tortured.”). See also Child Sexual Abuse Material (CSAM), NAT’L CTR. FOR MISSING & EXPLOITED CHILD. (Feb. 27, 2021), archived at https://perma.cc/4WRR-9UDB (citing a study from March 2018 that found girls appear in an overwhelming majority of abuse.
materials ("CSAM") have existed throughout history, their circulation has grown exponentially in the last decade.\(^3\) In response, tech companies, law enforcement agencies, and politicians have come together to pass legislation to combat the problem.\(^4\)

In 2008, the Providing Resources, Officers, and Technology to Eradicate Cyber Threats to Our Children Act ("PROTECT Our Children Act") passed to thwart CSAM on the internet, but was largely ineffective.\(^5\) In response, the Senate Judiciary Committee introduced the Eliminating Abusive and Rampant Technologies Act ("EARN IT Act") in March 2020.\(^6\) EARN IT was created to encourage and incentivize tech companies to take CSAM more seriously.\(^7\) In doing

\(^3\) See Keller & Dance, supra note 1 (citing that over a decade ago, "the proliferation of explicit imagery had already reached a crisis point" when the reported number was less than one million). See also Michael Salter, Child Sexual Abuse Materials: Another Global Pandemic, ISSTD NEWS (July 29, 2020), archived at https://perma.cc/5AKZ-VG2B (noting that in the last decade, reports of CSAM to authorities increased by fifty percent per year); Encryption trend threatens child safety gains, THORN (Nov. 19, 2020), archived at https://perma.cc/MU88-QSIZ (recognizing that there has been a 15,000% growth of child sexual abuse material in the past 15 years).

\(^4\) See Press Release, Debbie Wasserman Schultz, House of Representatives, Wasserman Schultz Celebrates PROTECT Act Reauthorization (Nov. 3, 2017), archived at https://perma.cc/75HT-W5BE (explaining that the law passed in 2008 organized a task force of federal, state, and local law enforcement and prosecutorial agencies to participate in investigations regarding child sexual exploitation online). See also Keller & Dance, supra note 1 (citing "landmark legislation" passed in 2008 after tech companies, law enforcement agencies, and legislators came together to control the problem).


\(^7\) See Introduce EARN IT Act, supra note 6 (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).”).
so, the EARN IT Act would establish a national commission to recommend best practices for identifying and reporting online exploitation. Additionally, the national commission would allow for Congressional review of best practices, liability safe harbors for compliant companies, and recourse for survivors. The suggested “best practices,” however, have left many wondering if they allow law enforcement unfettered access to innocent civilians’ private communications on social media platforms.

Child sexual exploitation is a serious problem that has been exacerbated by the Internet, which provides abusers widespread and quicker access to potential victims and anonymous platforms. Social media gives abusers ways to connect, which tech companies are largely ignoring. In the past, the federal government has worked with tech companies and law enforcement to address the problem. Legislation thus far has been largely ineffective, given the size of the problem, as well as lack of follow through and accountability on the part of government and law enforcement. The EARN IT Act, attempts to hold tech companies accountable for CSAM on their sites. The specific provisions may authorize technology companies to search citizens’ private communications.

II. History

A. Roots of CSAM

CSAM is not a novel issue, but the Internet gave abusers a platform to connect with others, to share materials, and to find victims. While the Internet exacerbated the problem, it has existed since Greek and Roman times, when young children were sexualized.

---

8 See id. (explaining the specifics of the EARN IT Act which included incentivizing tech companies to take this problem seriously, establishing a national commission, allowing for congressional review of best practices, creating safe harbors for liability, and providing recourse for survivors). 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).

9 See Introduce EARN IT Act, supra note 6 (enumerating the highlights of the EARN IT Act to explain the main goals of the proposed legislation and how they will improve upon the current remedies).

10 See Karr, supra note 8 (expressing concerns that the EARN IT Act could violate constitutional rights and diminish internet users’ privacy).

11 See Keller & Dance, supra note 1 (stating that child pornography predates the digital era).
through art and writing.\textsuperscript{12} The invention of the camera in 1826 gave rise to the modern concept of “child pornography.”\textsuperscript{13} The production of CSAM slowed until the 1960s, when societal attitudes toward censorship and sexual values turned increasingly liberal.\textsuperscript{14} In the 1970s, the demand for several child abuse films and magazines grew.\textsuperscript{15} Distribution of CSAM, however, was difficult as law enforcement could easily apprehend offenders.\textsuperscript{16}

The market for CSAM exploded with the Internet, which changed the fundamental ways the market functioned.\textsuperscript{17} Abusers created anonymous communities which provided easy and constant access to each other, as well as free material.\textsuperscript{18} Messenger applications

\textsuperscript{12}See 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 6 (2019) (stating that the sexualization of youth has always been present and that it was common in popular Greek and Roman writings).

\textsuperscript{13}See id. (stating that the invention of the camera in 1826 created the modern idea of child sexual exploitation).

\textsuperscript{14}See id. (citing a renewed sexualization of children in the 1960s due to “increased social liberalization and relaxation of censorship laws and sexual values . . .”).

\textsuperscript{15}See id. (stating that the 1970s “saw the release of several ‘classic’ child abuse films and more than 250 child sexual exploitation magazines in circulation across the United States”). While there was high interest, child pornography was difficult to obtain as magazines and videos were imported to the United States. Id. Magazines sold for $6 to $12 a piece and videos sold for $25 to $50 a piece. Id. See also The Online Marketplace for Child Sexual Abuse Materials, BERKLEY ECON. REV. (Dec. 4, 2019), archived at https://perma.cc/39PJ-MAQG (explaining that “[p]rior to the digital age, pornography was sold and distributed mainly through mail-order systems or from independent stores in the forms of magazines, books, standalone photographs, or video recordings”).

\textsuperscript{16}See Westlake, supra note 12, at 6 (citing the high cost and high chance of being apprehended by Customs or the Postal Service as slowing the spread of CSAM). At this time, it was more difficult for people to get in touch with each other than in modern times. Id. Because of this, child sexual exploitation was considered a “solitary crime with very sparse networks.” Id.

\textsuperscript{17}See id. (stating that with the advent of the internet, offenders were able to create online communities where they could connect). See also The Online Marketplace for Child Sexual Abuse Material, supra note 15 (noting that the internet changed the way materials could be viewed leaving no trace of activity).

\textsuperscript{18}See Westlake, supra note 12, at 6 (explaining that offenders were able to communicate with each other through online communities and “have 24/7, mostly anonymous and free, instant access, with better quality content and reduced risk of being apprehended . . .”). See also The Online Marketplace for Child Sexual Abuse
were a popular platform which developed into peer-to-peer sharing networks such as Gnutella.\footnote{See Westlake, supra note 12, at 7 (noting that as methods of transmitting files evolved, abusers went from Internet Relay Chat (messenger applications) to large peer-to-peer software networks like Gnutella). See also Gnutella, TECHOPEDIA (Apr. 25, 2020), archived at https://perma.cc/8BX6-B7DL (explaining that Gnutella is a “decentralized peer-to-peer (P2P) network that allows users to share files across the Internet without having to use a central server.”). Gnutella was propelled to success in 2001 when LimeWire basic became its first open-source client. Id.} This problem increased throughout the 1990s and early 2000s as mobile devices, search engines, file sharing, social networking, and messaging developed.\footnote{See Westlake, supra note 12, at 6 (citing technological advancements in the internet, including “search engines, peer-to-peer file sharing, instant messaging, and social networking” as solidifying the internet as the primary place to create and distribute child pornography).} With the rapid growth of technology, abusers gained easier access to victims and illegal materials.\footnote{See id. at 21 (explaining that the prevalence of cellular phones in adolescents has led to many creating their own content which is then found and redistributed by adults).}

In 2018, there were 18.4 million reports of CSAM which included over 45 million images and videos.\footnote{See Keller & Dance, supra note 1 (citing that in 2018, there were 18.4 million reports of child sexual abuse imagery). This number has grown exponentially over the previous 20 years with 3,000 reports in 1998; 100,000 reports over a decade later; and over 1 million in 2014. Id.} This global problem takes root in the United States as tech companies, headquartered primarily in Silicon Valley, play an integral role in facilitating the spread of CSAM throughout the world by failing to manage CSAM.\footnote{See id. (noting the global scope of the problem as most images were traced to other countries, but citing Silicon Valley as having a central role in facilitating the spread and reporting it to the authorities). Smartphone cameras, social media, and cloud storages are cited as allowing child abuse images to multiply at an alarming rate. Id. See also Tom Porter, Facebook reported more than 20 million child sexual abuse images in 2020, more than any other company, INSIDER (Feb. 26, 2021), archived at https://perma.cc/Q6ZG-3S9Y (emphasizing that “[t]here are no laws in the US compelling platforms to proactively search out child sexual abuse material.”).} Social networking sites made it possible to find victims and other abusers to make and circulate new content.\footnote{See Westlake, supra note 12, at 7 (stating that internet platforms have created communities of offenders, including Blogger, LiveJournal, and Tumblr).} Although much of CSAM circulates on the dark web, it exists on all platforms, including
mainstream sites. Some child abuse groups utilize encryption and the dark web to share images of extreme abuse and teach others how to do the same. Given the explosion of CSAM on the Internet and creative routes abusers utilize, the circulation of CSAM has become difficult for law enforcement to manage.

In 2020, the COVID-19 pandemic created a spike in CSAM. The pandemic forced millions in their homes to avoid spreading the virus, and left many victims vulnerable and isolated with abusers. The closure of schools, restrictions on international travel, and increased time on online created ripe circumstances for abusers. In

---

25 See Keller & Dance, supra note 1 (explaining that child abuse images occupy “all corners of the internet,” including Facebook Messenger, Dropbox, and Bing).
26 See id. (stating that some online groups devote themselves to extreme forms of abuse, sometimes on younger children, and utilize encryption and the dark web to promote their tactics and encourage others to join).
27 See id. (noting that law enforcement agencies across the country feel “besieged” and have to prioritize their workload by focusing on images depicting young victims). See also Daniel Malan, The law can’t keep up with new tech. Here’s how to close the gap, WORLD ECON. F. (June 21, 2018), archived at https://perma.cc/74PH-S74B (explaining that economic actors and regulators play a cat-and-mouse game when it comes to enforcement of law and new technologies).
29 See Butler, supra note 28 (explaining that many victims have been trapped with their abusers during COVID-19). See also INTERPOL report highlights impact of COVID-19 on child sexual abuse, INTERPOL (Sept. 7, 2020), archived at https://perma.cc/Y7JL-XF43 (citing social and economic factor changes because of COVID-19 that have impacted child sexual exploitation and abuse across the world).
30 See Butler, supra note 28 (citing “closure of schools, restrictions on international travel, and an increased amount of time spent online” as creating the “perfect storm” for predators). See also INTERPOL report highlights impact of COVID-19 on child sexual abuse, supra note 29 (citing the closure of schools, increased time online, restriction of international travel, and limited access to community support services as obstacles for victims getting help during the pandemic); COVID-19 restrictions
September 2020, The International Criminal Police Organization ("INTERPOL") released a report that noted increases in the amount of CSAM shared on peer-to-peer networks, the dark net, and self-generated materials. The report cites more time spent at home, economic hardships, and opportunities for abuse as significant factors in the overall increase. Officials call this recent surge “just the tip of a growing iceberg.”

B. The U.S. Government & Law Enforcement Response

In 2008, the “PROTECT Our Children Act” was passed. This Act was a created a task force allowing law enforcement to expand its ability to investigate, apprehend, and prosecute abusers. Despite the comprehensive efforts of the legislation, CSAM continued to expand. An investigation by the New York Times revealed several issues including understaffed and underfunded law enforcement agencies, neglect on the part of the Justice Department, and a failure
of tech companies to report violations to law enforcement.\textsuperscript{37} Lack of consistent communication and cooperation between law enforcement, the federal government, and tech companies has been a hindrance to investigating, catching, and prosecuting abusers.\textsuperscript{38}

The federal government neglected many obligations under the PROTECT Our Children Act.\textsuperscript{39} In 2019, the Justice Department published only two of the six required reports under the legislation.\textsuperscript{40}

\textsuperscript{37} See Ali Breland, \textit{Online Content Depicting Child Sexual Abuse Is Growing at an Alarming Rate}, MOTHER JONES (Sept. 29, 2019), archived at https://perma.cc/77MG-QT2R (noting that law enforcement agencies report that they are understaffed and underfunded). \textit{See also} Josh Sweigart, \textit{Increased child porn reports stretch police resources in Ohio}, THE ALL. REV. (Mar. 14, 2020), archived at https://perma.cc/6CFS-WXGU (explaining that an investigation in Ohio revealed that law enforcement agencies in their state raised concerns they did not have enough resources to handle the recent increase in online child sexual abuse reports); Keller & Dance, \textit{supra} note 1 (outlining some of the problems discovered in The New York Times investigation as to why the child abuse content increased after new legislation was passed).

\textsuperscript{38} See Bloomberg, \textit{Police Are Increasingly Asking Tech Companies for Digital Evidence on Mobile Phones and Apps}, FORTUNE (July 25, 2018), archived at https://perma.cc/TD58-LD9U (explaining a study conducted through surveys and interviews with law enforcement officials about the challenges law enforcement faces in accessing digital evidence).

Thirty percent of law enforcement respondents said their department had trouble identifying which service providers have access to digital evidence they want, and 25 percent cited difficulty obtaining relevant digital evidence from providers once the right company was identified . . . police agencies’ lack of knowledge about digital evidence can lead to requests for information that seem overly broad to tech companies. \textit{Id. See also} Keller & Dance, \textit{supra} note 1 (noting that tech companies are not required to look for child abuse images but just to report them when they are found); WESTLAKE, \textit{supra} note 12, at 13 (explaining that “[i]nvestigating child sexual exploitation . . . is difficult due to the lack of cooperation between government bodies . . . ”).

\textsuperscript{39} See Keller & Dance, \textit{supra} note 1 (stating that while the PROTECT Our Children Act anticipated many of the modern problems, the federal government has not cooperated with many aspects of the legislation).

\textsuperscript{40} See John Sciamanna, \textit{Child Sexual Abuse is More Accessible Today Because of the Internet}, CWLA (Feb. 28, 2021), archived at https://perma.cc/625V-ZEEB (explaining that upon learning of the federal government’s failures under the legislation, Congresswoman Debbie Wasserman Schultz sent a letter to then Attorney General William Barr). \textit{See also} Keller & Dance, \textit{supra} note 1 (citing that only two of six required reports have been produced and that there have been constant short-term appointees to lead the department).
Many felt as if the task force created under the legislation was not a priority.41 The legislative efforts were underfunded, making efforts to follow through on obligations futile.42 Responding agencies were unable to hire enough agents and prosecutors to keep up with the number of cases.43 Ultimately, many of the failures under the legislation came down to lack of communication between the federal government and law enforcement.44

The lack of communication extended further to cooperation issues between tech companies and law enforcement.45 Tech companies are not required to monitor their platforms for child abuse images and are only required to report discovered materials.46 Often, companies will only respond to law enforcement inquiries to state they no longer have any relevant record(s).47 While the dark web and peer-to-peer file sharing are preferred methods of disseminating CSAM, the second most popular mode of acquiring child abuse materials is the

41 See id. (quoting Francey Hakes, former leader of the internet crimes against children department, saying that no one “felt like the position was as important as it was written by Congress to be.”).

42 See id. (noting that the federal government has not fulfilled its funding goals). Additionally, in 2019, the Department of Homeland Security lost six million dollars from cybercrimes units to immigration enforcement. Id. A survivor who testified in support of the legislation noted that although the bill passed, it has not been funded. Id.

43 See Michael H. Keller, A $5 Billion Proposal to Fight Online Child Sexual Abuse, THE N.Y. TIMES (May 5, 2020), archived at https://perma.cc/66T8-5QBU (explaining that more funding would allow organizations to increase their staff in order to keep up with the growing number of cases).

44 See Keller & Dance, supra note 1 (noting that an author of the PROTECT Our Children Act, Representative Debbie Wasserman Schultz, was unaware that the federal government had failed to meet their obligations under the legislation).

45 See Miriam Jones, How Social Media is Changing Law Enforcement, GOVTech (Dec. 2, 2011), archived at https://perma.cc/CKT8-WUL4 (explaining that the biggest problem for local law enforcement involves obtaining and retaining social media records during investigations). See also Keller & Dance, supra note 1 (stating that police records show that tech companies can take weeks or months to respond to inquiries from law enforcement, if they respond at all).

46 See id. (stating that after weeks or months of waiting, tech companies sometimes only respond to say they do not have any records). Additionally, tech companies are only legally required to report images that have been discovered. Id.

47 See Jose Pagliery, Tech companies are hindering criminal investigations, under outdated law, CNN BUS. (Oct. 19, 2017), archived at https://perma.cc/BZX6-EEL3 (noting a case where state investigators could not access the emails of a defendant to help identify victimized children). Google refused to give information to law enforcement despite a warrant, claiming that the data was out of its jurisdiction. Id.
surface web. Unlike the dark web, which is only accessible via certain browsers, the surface web hosts content available to the general public. Encryption is a serious hindrance to law enforcement investigations of CSAM. Encryption takes readable text and scrambles it, so that it can only be deciphered by a person who has the decryption key. Encryption addresses many serious and legitimate privacy concerns, as it can be used to protect anything from text messages to bank account information. It is often used to guard

48 See Westlake, supra note 12, at 7 (citing the surface web as a “popular locale for [Child Sexual Exploitation Material]” and that the World Wide Web, or public websites, is the second most popular mode of acquiring child abuse imagery).

49 See Dark Web, PCMag (Mar. 29, 2021), archived at https://perma.cc/D76F-7C4F (defining the “dark web” as “[a] file sharing network used to illegally distribute . . . nefarious documents.”). Additionally, the dark web is “[a] part of the ‘deep Web’ that is only accessible via browsers such as Tor, which stands for ‘The Onion Router.’” Id. See also Surface Web, PCMag (Mar. 29, 2021), archived at https://perma.cc/KW6Y-R8NV (defining the surface Web as “[c]ontent on the World Wide Web that is available to the general public.”). Additionally, the surface Web is “indexed by the major search engines . . . .” Id.

50 See What Concerns do the FBI and the law enforcement communities have regarding the growing use of encryption products by the public, both domestically and abroad?, FBI (Feb. 27, 2021), archived at https://perma.cc/3Y5P-9XBW (explaining that law enforcement is concerned about the threat posed by “the use of robust encryption products that do not allow for authorized access or the timely decryption of critical evidence, obtained through lawful electronic surveillance and search and seizure.”). See also Lawful Access, The U.S. Dep’t of Just. (Oct. 30, 2020), archived at https://perma.cc/AQ2W-F99Z (noting that warrant-proof encryption can provide a “‘lawless space’ that criminals, terrorists, and other bad actors can exploit”); Keller & Dance, supra note 1 (noting that even when tech companies do cooperate with law enforcement, “encryption and anonymization can create digital hiding places for perpetrators.”).

51 See Alison Grace Johansen, What is encryption and how does it protect your data?, NortonLifeLock (July 24, 2020), archived at https://perma.cc/AS4Z-2YJZ (explaining how the process of encryption works). See also Privacy Guy, What is Encryption & How Does it Work?, Internet Priv. Guy (Nov. 27, 2020), archived at https://perma.cc/HS6N-Y83T (explaining that “[b]asic forms of encryption may be as simple as switching letters.”). “Encryption uses algorithms to scramble your information. It is then transmitted to the receiving party who is able to decode the message with a key.” Id.

52 See Johansen, supra note 51 (explaining the type of information that encryption can protect). See also Ryan Polk & April Froncek, Your Day with Encryption, Internet Soc’y (Oct. 22, 2019), archived at https://perma.cc/4J7X-J62B (walking through how encryption is used for everyday events such as online shopping, mobile banking, and secure messaging apps).
information from hackers.\textsuperscript{53} Both the sender and the recipient must use the encryption key to unlock the information, which law enforcement does not have access to.\textsuperscript{54} In March 2019, Mark Zuckerberg announced Facebook’s plan to encrypt its messenger service, which alone was responsible for nearly 12 million reports of CSAM.\textsuperscript{55} Encryption has become an increasingly popular way to distribute child pornography for criminals as the anonymity keeps them steps ahead of police.\textsuperscript{56} The anonymity of encryption not only makes it harder for law enforcement to investigate, but emboldens anonymous abusers to post more frightening imagery.\textsuperscript{57} The use of end-to-end encryption by sites like Facebook could have dangerous ramifications.\textsuperscript{58}

\textsuperscript{53} See Johansen, supra note 51 (enumerating the advantages to encryption which include fending off hackers who are looking to steal people’s person information). See also 6 Ways to Protect Yourself From Hackers, CHUBB (Feb. 6, 2022), archived at https://perma.cc/8DAG-3PSU (citing the storage encryption feature on your phone as a way to protect your private data from hackers).

\textsuperscript{54} See Johansen, supra note 51 (explaining how encryption works in communications between two or more people).

\textsuperscript{55} See Casey Newton, Mark Zuckerberg says Facebook will shift to emphasize encrypted ephemeral messages, THE VERGE (Mar. 6, 2019), archived at https://perma.cc/GD5G-ND78 (announcing Facebook’s plan to shift its communications to private, encrypted services); Elizabeth Dwoskin, Facebook’s Mark Zuckerberg says he’ll reorient the company toward encryption and privacy, THE WASH. POST (Mar. 6, 2019), archived at https://perma.cc/3JCH-CXZ8 (noting that Zuckerberg announced the plan to switch to encryption in a lengthy essay on his own Facebook account which focused on user privacy). See also Andy Greenberg, Facebook Says Encrypting Messenger by Default Will Take Years, WIRED (Jan. 10, 2020), archived at https://perma.cc/FX89-68AF (explaining that Mark Zuckerberg pledged Facebook would apply end-to-end user communications across all of its platforms in order to grant strong new protections to over a billion users).

\textsuperscript{56} See Katrina Sabados, Encryption: A Godsend to All Who Seek Privacy, Even Criminals, ORGANIZED CRIME & CORRUPTION REPORTING PROJECT (Oct. 31, 2019), archived at https://perma.cc/ET7S-NYTD (explaining how a drug cartel used encrypted text messages to evade law enforcement); Keller & Dance, supra note 1 (citing that criminals used advanced technologies such as encryption to stay ahead of police).

\textsuperscript{57} See Ryan Browne, Google, Facebook and Microsoft back global plan to ‘eradicate’ online child sexual abuse, CNBC (June 12, 2020), archived at https://perma.cc/SC68-EW2Y (explaining that tech companies and law enforcement have clashed over the use of encryption in online messaging services). See also Keller & Dance, supra note 1 (stating that “anonymity offered by the sites emboldens members to post images of very young children being sexually abused, and in increasingly extreme and violent forms.”).

\textsuperscript{58} See Kris Holt, DOJ asks Facebook to halt end-to-end encryption plans (updated), ENGADGET (Oct. 3, 2019), archived at https://perma.cc/85HU-9RGH (explaining
While tech companies have made progress in reporting child abuse material, many see these efforts as too late.59 For years companies were aware of CSAM, but for unclear reasons, chose not to address the issue.60 Delayed reporting from companies made it difficult for law enforcement to investigate cases, as crucial evidence was no longer available.61 One of the most problematic companies is the blogging website, Tumblr.62 Many Tumblr users reported seeing that the DOJ expressed concern to Facebook in light of the encryption announcement that it would “hamper law enforcement from tackling illegal activity that occurs through Facebook’s messaging platforms.”). In addition to child sexual exploitation, the DOJ also cited terrorism and election meddling as a concern. *Id.* See also Keller & Dance, *supra* note 1 (stating, “Facebook’s plans to encrypt Messenger in the coming years will lead to vast numbers of images of child abuse going undetected.”). Mark Zuckerberg, the CEO of Facebook, acknowledged that encrypting messenger did in fact present a risk for child exploitation. *Id.*

59 See Leah Rodriguez, *Tech Companies Are Failing to Stop Online Sexual Abuse, NYT Report Reveals, GLOB. CITIZEN* (Nov. 15, 2019), archived at https://perma.cc/3C7R-A4WG (explaining that major tech companies have failed to stop the circulation of CSAM on their platforms). See also Keller & Dance, *supra* note 1 (quoting a former federal prosecutor who said, “[t]he recent surge by tech companies in filing reports of online abuse ‘wouldn’t exist if they did their job then.’”).

60 See *id.* (asserting, “companies have known for years that their platforms were being co-opted by predators, but many of them essentially looked the other way.”). As a result of this neglect, when they did come around to investigating the problem, it was worse than they could have imagined. *Id.*

61 See Information for Law Enforcement Authorities, FACEBOOK SAFETY CTR. (Feb. 28, 2021), archived at https://perma.cc/7B59-KUDN (explaining that Facebook preserves account records in connection with official criminal investigations for 90 days pending Facebook’s receipt of formal legal process). See also Keller & Dance, *supra* note 1 (stating, “[f]ederal law requires companies to preserve material about their reports of abuse imagery for 90 days.”). Due to the large number of reports and requests for data, sometimes companies reach out to authorities when it is already too late. *Id.*

62 See Cassidy Dawn Graves, *Tumblr Users Spent Years Reporting Child Porn. They Say the Site Ignored Them., MEL* (Feb. 28, 2021), archived at https://perma.cc/PT7M-RW7G (explaining the experiences of Tumblr users who attempted to report child sexual abuse images but were unsuccessful due to logistical problems). See also Keller & Dance, *supra* note 1 (citing an investigation of Tumblr stalling for over a year, as well as another case in which the company alerted the reported account it was under investigation, which allowed him to destroy the evidence).
CSAM frequently with no way to report them.\textsuperscript{63} Other problematic companies include the search engine, Bing and photo sharing app, Snapchat.\textsuperscript{64} Snapchat is particularly problematic as communications disappear after a certain amount of time, hindering investigations.\textsuperscript{65} Fewer than two percent of crimes being investigated as a result of poor communication from tech companies.\textsuperscript{66}

In addition to a spike in abuse materials, the pandemic has made it more difficult for law enforcement to track abusers.\textsuperscript{67} Additionally, there have been more delays in reporting.\textsuperscript{68} Downsizing measures and staff cutbacks have also impeded police efforts.\textsuperscript{69}

\textsuperscript{63}See Graves, supra note 62 (explaining a Tumblr user’s experience in coming across child sexual abuse imagery). One user found that the email indicated for reporting these images was no longer even in use. Id.

\textsuperscript{64}See Jeremy Hobson, Snapchat ‘Has Become A Haven’ For Child Predators, Criminal Justice Scholar Says, WBUR (Jan. 23, 2018), archived at https://perma.cc/D2KA-2UFT (explaining how it is difficult for investigators to gather evidence from Snapchat because the photos and messages disappear). See also Keller & Dance, supra note 1 (stating that Bing submitted reports that lacked essential information and hindered investigations, while Snapchat often failed to provide any information to law enforcement given that the platform deletes its own contact in a short period of time).

\textsuperscript{65}See Hobson, supra note 64 (interviewing Professor Adam Scott Wandt who stated, “Snapchat has become a haven for child predators” as they can “induce children to send pictures of them[elves].”). Because these photos disappear after a certain period of time, it is difficult for law enforcement to investigate reports. Id.

\textsuperscript{66}See Keller & Dance, supra note 1 (quoting a criminal investigator who predicted that “fewer than two percent of crimes would be investigated” due to law enforcement task forces being overwhelmed and underfunded). See also Ishan Mehta, The Need for Better Metrics on Cybercrime, THIRD WAY (Oct. 1, 2019), archived at https://perma.cc/9KVL-YLZC (estimating that based on available data, “less than 1% of cyber incidents see an arrest of the perpetrator”).

\textsuperscript{67}See Butler, supra note 28 (noting that the pandemic has created a spike in abuse materials and an inability of law enforcement to keep up).

\textsuperscript{68}See INTERPOL report highlights impact of COVID-19 on child sexual abuse, supra note 29 (explaining that the pandemic has created delayed reporting of abuse). See also INTERPOL, THREATS AND TRENDS CHILD SEXUAL EXPLOITATION AND ABUSE: COVID-19 IMPACT 7 (2020) (noting that “60 percent of member countries who regularly use the [International Child Sexual Exploitation] database have either not accessed the database or have seen a significant reduction in their activities during the COVID-19 pandemic.”).

\textsuperscript{69}See Rebecca Rainey & Maya King, Defund the police? It’s already happening thanks to the Covid-19 budget crunch, POLITICO (Aug. 15, 2020), archived at https://perma.cc/KC6R-JXYN (explaining that the coronavirus depleted police budgets).

The squeeze is happening nationwide: Seattle’s City Council on Monday approved nearly $3 million in cuts from the Seattle Police
Working from home, the processes of investigation, and general efficiency of reporting efforts have made investigations even more complex. Notably, courts closed during the pandemic, delaying the ability to process cases.

C. Section 230 and its Impact on Technology Companies

Big tech companies, such as Facebook, Google, Bing, and Tumblr, are afforded legal immunity for criminal activity on their platforms under Section 230 of the 1996 Communications Decency Act (“CDA”). The CDA is a portion of the Telecommunications Act of 1996 and was aimed at addressing concerns regarding minors’ access to pornography on the internet. Section 230 Immunity was meant to allow freedom of expression online without putting the burden of
policing speech on tech companies. While the Communications Decency Act was aimed at restricting unfettered free speech on the Internet, it included Section 230 as a seemingly contradictory provision, to protect freedom of expression and innovation.

While anti-free speech provisions were struck down by the Supreme Court, Section 230 remains an important law. The section protects online sites from laws that would hold them legally responsible for users’ actions and words. Section 230 allows personal videos to be posted on YouTube, product reviews to be posted on retail sites, and individuals’ thoughts and opinions to be expressed on Facebook. This section also shields tech companies from liability for their role in the spread of child abuse imagery. Despite Section 230 immunity, tech companies do produce information for eighty percent of law enforcement requests. Tech companies have a

74 See Rodrigo, supra note 72 (explaining that the internet association expressed fears that changes to the Section 230 immunity would severely limit user’s ability to express themselves online).
75 See CDA 230: The Most Important Law Protecting Internet Speech, ELEC. FRONTIER FOUND. (Oct. 18, 2020), archived at https://perma.cc/UP5T-TQJ4 (stating that Section 230 is “one of the most valuable tools for protecting freedom of expression and innovation on the Internet” despite the fact that the purpose of the legislation was to restrict free speech on internet platforms).
76 See id. (stating that the anti-free speech provisions were struck down by the Supreme Court, but that Section 230 continues).
77 See id. (explaining exactly what Section 230 entails). See also Ryan Mrazik & Natasha Amlani, Cover Story on Section 230: A Law on the Cusp of Change?, 35 ANTITRUST A.B.A. 26, 26 (2020) (explaining that the CDA establishes that “service providers are not liable for (1) communications or content posted by people who use their services, (2) their services’ design or structure, or whether and how to allow people to have accounts, and (3) discretionary decisions about removing or restricting access to certain objectionable content.”).
78 See CDA 230: The Most Important Law Protecting Internet Speech, supra note 75 (explaining the protections Section 230 offers to certain online platforms that allow them to function).
79 See Mrazik & Amlani, supra note 77 (explaining that before the EARN IT Act was introduced, service providers were able to assert CDA immunity from criminal or civil lawsuits under state laws for advertising, promoting, presenting, or soliciting CSAM).
80 See Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance, 131 HARV. L. REV. 1722, 1722 (2018) (stating that in 2017 Facebook, Google, and Twitter responded to approximately eighty percent of law enforcement requests for records). Additionally, tech companies act as “surveillance intermediaries,” meaning that they “sit between law enforcement agencies and the public’s personal information.” Id. See also Ella Fassler, Here’s How Easy It Is for Cops to Get Your Facebook Data, ONEZERO (June 17, 2020), archived at
discretion in determining what information the government has access to.\(^{81}\)

**D. Fourth Amendment Search and Seizure Principles**

The Fourth Amendment protects citizens from unreasonable searches and seizures of a protected area by the government.\(^{82}\) In order for a search of a protected class to be reasonable, the government must obtain a warrant supported by probable cause.\(^{83}\) Whether the government must establish probable cause and obtain a warrant depends on the nature of the items searched.\(^{84}\) Early notions of

---

https://perma.cc/EEW7-9NH6 (citing a statistic that “Facebook provided law enforcement with data in 88% of cases in 2019.”). See also TheBestVPN LTD., Can the Police Use Facebook to Investigate Crimes?, GOVTech (Mar. 5, 2017), archived at https://perma.cc/WGB3-N8EE (explaining that a 2012 survey found that 80% of law enforcement officials used social media to assist in investigations).

81 See Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance, supra note 80, at 1723 (stating that tech companies determine, in part, the government’s access to information including, but not limited to, “personal relationships, professional engagements, travel patterns, financial circumstances”).

82 See U.S. CONST. amend. IV, § 1 (laying out the protections under the Fourth Amendment).

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Id. See also James C. English, Sobriety Checkpoints Under State Constitutions: What Has Happened to Sitz?, 59 U. PITT. L. REV. 453, 456 (1998) (explaining that “[w]hether a search or seizure is consistent with the Fourth Amendment hinges on whether it is reasonable.”).

83 See id. (stating in relevant part that “no Warrant shall issue, but upon probable cause, supported by Oath or affirmation . . . .”). See also Tracey Maclin, Katz, Kyllo, and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century, 72 Miss. L. J. 51, 52 (2002) (explaining “[t]he Fourth Amendment proscribed intrusions into a home unless a government official obtained a judicial warrant supported by specific procedural safeguards.”).

84 See English, supra note 82, at 456 (stating in relevant part that the Fourth Amendment protects “persons, houses, papers, and effects, against unreasonable searches”). See also Andrew Guthrie Ferguson, The Internet of Things and the Fourth Amendment of Effects, 104 CALIF. L. REV. 805, 808 (2016) (explaining how the understanding of “persons, houses, papers, and effects” has evolved overtime). “‘[E]ffects’ . . . are no longer just inactive, static objects, but objects that create and communicate data with other things.” Id.
unreasonable searches included physical trespass and tangible items being seized. This idea evolved with the *Katz v. United States* decision, holding anything that a person knowingly exposed to the public is not protected from search and seizure. Further, under the third-party doctrine set forth in *United States v. Miller* and *Smith v. Maryland*, there is no reasonable expectation of privacy in records held by a third-party.

In 2018, the Supreme Court pivoted from traditional Fourth Amendment privacy notions, holding that the government must obtain a warrant to search Cell Site Location Information (“CSLI”).

---

85 See *History and Scope of the Amendment*, CORNELL L. SCH.: LEGAL INFO. INST. (Jan. 30, 2021), archived at https://perma.cc/GQ2Z-UADG (explaining that the Court initially held that wiretapping was not covered by the Amendment because there was no physical trespass involved). See also Robert C. Power, *Criminal Law: Technology and the Fourth Amendment: A Proposed Formulation for Visual Searches*, 80 J. CRIM. L. & CRIMINOLOGY 1, 3 (1989) (explaining that “[f]or most of the nation’s history, the courts treated that amendment as regulating only ‘physical’ searches and ‘tangible’ seizures.”). See generally *Olmstead v. United States*, 277 U.S. 438, 466 (1928) (holding a physical trespass is needed to be considered a search and that seizure must include tangible items as described in the Fourth Amendment of the Constitution).

86 See *Katz v. United States*, 389 U.S. 347, 351 (1967) (holding that because the Fourth Amendment “protects people, not places,” if a person knowingly exposes something to the public, even in a private location, is not subject to protection). Additionally, what a person “seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.” Id. See also *Kyllo v. United States*, 533 U.S. 27, 34–35 (2001) (holding that any information obtained by the police with the help of advanced technology, which could not have otherwise been seen without entering into one’s home, is a breach of privacy); Power, supra note 85, at 3 (explaining that “the Supreme Court changed its approach to evaluating searches and seizures” in 1967 with the *Katz* decision).

87 See *United States v. Miller*, 425 U.S. 435, 446 (1976) (holding that there was no Fourth Amendment interest in bank records). See also *Smith v. Maryland*, 442 U.S. 735, 745 (1979) (holding that there was no actual expectation of privacy in the phone numbers dialed and therefore tracking those numbers was not a search); *California v. Greenwood*, 486 U.S. 35, 40 (1988) (holding that there is no right to privacy in something you give to a third party or that is readily observable by police).

88 See *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018) (holding that the fact that the government obtained the CSLI from a third-party does not overcome the claim to Fourth Amendment protection). See also *Riley v. California*, 573 U.S. 373, 407 (2014) (holding that when a cell phone is seized as a search incident to arrest, a warrant is necessary to search the digital contents of the cell phone); Samuel D. Thomas, *Collect Call For Clarification: How Carpenter Has (And Has Not) Changed Modern Fourth Amendment Jurisprudence*, 60 B.C. L. REV. 2221, 2224 (2019) (explaining how the Court reinterpreted Fourth Amendment doctrines in *Carpenter*); H. Rick Yelton, *Riley v. California: Setting the Stage For the Future of*
this information fails traditional tests of search and seizure case law, the Court held that because CSLI was so “deeply revealing,” a warrant was necessary to obtain such information.\(^8^9\) Given that social media accounts are becoming as prevalent in modern life as cell phones, it is significant to consider the implications of this case.\(^9^0\)

While a Fourth Amendment search and seizure is generally considered to be performed by law enforcement, private citizens can act as government agents.\(^9^1\) If a private citizen acts on their own in searching a protected area, it is not in violation of the Fourth Amendment.\(^9^2\) When a private actor conducts a search of a protected area, it is not in violation of the Fourth Amendment.\(^9^3\) See United States v. Smith, 383 F.3d 700, 708 (8th Cir. 2004) (setting forth the test for determining whether a private citizen acted as an agent of law enforcement in conducting a search). See also United States v. Harling, 705 F. App’x 911, 916 (2017) (holding that the two private citizens were not government agents in conducting their own search of the defendant’s USB drive).
area under the direction of the government, however, that search is subject to protections.93

Another category of searches is a “special needs searches” which address vital problems that can only be addressed through a search and go beyond normal law enforcement purposes.94 These searches would be compromised if they were to require individualized suspicion, and therefore constitute an exception to the warrant requirement.95 The Supreme Court has held if there is a special, vital, problem that can be addressed using a search where probable cause or a warrant would undermine the government’s efforts, it is acceptable to perform the

93 See Edmonson v. Leesville Concrete Co., 500 U.S. 614, 620 (1991) (holding that private parties acting under governmental authority are subject to constitutional constraints). “Although the conduct of private parties lies beyond the Constitution’s scope in most instances, governmental authority may dominate an activity to such an extent that its participants must be deemed to act with the authority of the government and, as a result, be subject to constitutional constraints.” Id.

94 See Skinner v. Labor Exec. Ass’n, 489 U.S. 602, 609–10 (1989) (holding that searches of train conductors were appropriate to prevent trains being driven by employees under the influence of drugs or alcohol). See also Board of Ed. v. Earls, 536 U.S. 822, 830 (2002) (holding that drug testing students who wanted to participate in extracurricular activities was valid because students had limited privacy interests at school and the intrusion was minimal compared to the school’s interest in combatting the drug problem); Mich. Dep’t of State Police v. Sitz, 496 U.S. 444, 477 (1990) (Brennan, J., dissenting) (holding that a sobriety checkpoint program which stopped all vehicles passing through was justified as a search where there was a significant problem in detecting alcohol impaired drivers); Nat’l Treasury Emps. Union v. Von Raab, 816 F.2d 170, 178 (1987) (holding that drug testing programs for employees who carry firearms, are involved in intercepting drug importation, or are in high level positions involving classified information are justified in departing from ordinary warrant and probable cause requirement by the substantial government interest in stifling the drug trade). But see Chandler v. Miller, 520 U.S. 305, 318 (1997) (holding that drug testing program for state office candidates in Georgia was invalid where the government need was not substantial enough to justify foregoing individualized suspicion).

95 See Skinner, 489 U.S. at 634 (holding that this type of search was applicable where the probable cause and warrant requirements were not practicable to achieve the goal). See also Nat’l Treasury Emps. Union, 816 F.2d at 173 (holding that the government had a compelling interest in determining that employees were not involved in the consumption of illegal drugs and that the search did not require individualized suspicion).
search without a warrant. Special needs searches should be carefully considered in examining the best practices of the EARN It Act.

III. Facts

In January of 2020, the first draft of the EARN IT Act circulated. The Act looked to remove immunity for tech companies under Section 230 for CSAM circulation. Companies were required to comply with “best practices” that would later be determined. Under the first draft, the Attorney General (“AG”), had the ultimate power in determining the best practices. The Act has since been revised several times.

---

96 See Skinner, 489 U.S. at 631 (holding that where particularized suspicion is “unrealistic and inimical to the Government’s goal of ensuring safety,” it is acceptable to perform the search without it).

97 See Brian Mund, Social Media Searches and the Reasonable Expectation of Privacy, 19 Yale J. L. & Tech. 238, 240 (2017) (noting how “[i]nformation shared on social platforms may offer a valuable resource to government investigators.”).

98 See Alan Z. Rozenshtein, The Revised EARN IT Act Proposes a Better Profess 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).

99 See id. (giving a broad overview of the first draft of the EARN IT Act). See also Mark MacCarthy, Back to the Future for Section 230 Reform, LAWFARE (Mar. 2, 2021), archived at https://perma.cc/P4Q2-RMZY (explaining that the act “would withdraw Section 230 protection for violations of child sexual abuse laws.”).

100 See Rozenshtein, supra note 98 (explaining that best practices were not yet determined in the first draft of the act that was circulated).

101 See id. (noting the amount of power given to the Attorney General by the initial draft of the act).

102 See id. (explaining that the draft of the act formally introduced to the Senate in March contained “major revisions”). See also Emily Birnbbaum, Amendments to the EARN IT Act could resolve its encryption issues, PROTOCOL (July 1, 2020), archived at https://perma.cc/EBB2-T5EW (explaining that in July, a “manager’s amendment” to the act was published); Riana Pfefferkorn, THE EARN IT ACT THREATENS OUR ONLINE FREEDOMS. NEW AMENDMENTS DON’T FIX IT., THE CTR. FOR INTERNET AND SOC’Y (July 6, 2020), archived at https://perma.cc/92EX-H4DF (explaining further the manager’s amendment and the Leahy amendment in July of 2020).
A. Draft Introduced in the Senate

The EARN IT Act was introduced in the U.S. Senate on March 5, 2020. The Act was supported by a bipartisan coalition headed by Democratic Senator Richard Blumenthal and Republican Senator Lindsay Graham. The overall goal of the Act was to fight CSAM. EARN IT intended to hold tech companies accountable for the creation and distribution of CSAM. The initial draft of the EARN IT Act required tech companies to “earn” Section 230 immunity by following the Act’s “best practices”.

Under the first draft, the EARN IT Act established the National Commission on Online Child Sexual Exploitation Prevention, which would determine best practices tech companies have to follow. At the time of this was introduced, there were no uniform practices in place for tech companies to follow. The commission would consist

103 See Introduce EARN IT Act, supra note 6 (noting when the EARN IT Act was introduced in the Senate). See also Rozenshtein, supra note 98 (noting when the act was formally introduced to the Senate); Rebecca Kern, Internet Firms’ Liability Protection Under Fire. 26 Words and What’s at Stake, INS. J. (Mar. 4, 2021), archived at https://perma.cc/V4X8-4LUV (explaining that the act was introduced in the senate in March of 2020).
104 See Introduce EARN IT Act, supra note 6 (noting the bipartisan support the bill earned in the Senate Judiciary Committee). See also Kern, supra note 103 (noting how the act was introduced in the Senate in March 2020 and advanced by the Senate Judiciary Committee); 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).
105 See Dahan, supra note 104 (noting the overarching goal of the act).
106 See Introduce EARN IT Act, supra note 6 (explaining the goals of the EARN IT Act). See also Kern, supra note 103 (explaining that the act would “allow for state civil and criminal lawsuits as well as federal lawsuits if companies advertise, promote, present, distribute or solicit child sexual abuse material”); Stewart Baker, The Earn it Act Raises Good Questions About End-To-End Encryption, LAWFARE (Feb. 11, 2020), archived at https://perma.cc/ZM5N-G9QP (explaining that the act “would allow civil suits against companies that recklessly distribute child pornography.”).
107 See Dahan, supra note 104 (explaining that in the first draft, “internet companies needed to ‘earn’ the protections of Section 230.”).
108 See Rozenshtein, supra note 98 (noting that the act would set up a commission “to develop best practices that companies would have to adopt to get immunity.”). See also Dahan, supra note 104 (citing the name of the commission to be created by the bill).
109 See U.S. DEPT. OF JUSTICE, SECTION 230 – NURTURING INNOVATION OR FOSTERING UNACCOUNTABILITY? 1 (June 2020), archived at
of nineteen members. A spot would be reserved for the AG, Secretary of Homeland Security, and the Chairman of the Federal Trade Commission (“FTC”). The remaining sixteen spots would go to law enforcement, the community of child-exploitation victims, legal and technology experts, and tech companies. Those spots would be chosen by the leaders of each party from the House of Representatives and the Senate. The approval of fourteen members would be required for any best practices to be enacted. Approved best practices would then be subject to approval from the AG, Secretary of Homeland Security, and FTC Chairman. The AG would publish the best practices on the Department of Justice (“DOJ”) Website and the

https://perma.cc/EX9C-JNP8 (stating that the expansive interpretation of Section 230 by courts “has left online platforms both immune for a wide array of illicit activity on their services and free to moderate content with little transparency or accountability.”).

110 See Dahan, supra note 104 (explaining the make-up of the commission). See also Rozenshtein, supra note 98 (giving a detailed explanation of the 19-member commission under the bill).

111 See id. (explaining that “[t]hree spots would be reserved for the attorney general, the secretary of homeland security and the chairman of the Federal Trade Commission.”). See also Dahan, supra note 104 (noting the commission “would be formed by three agency heads: the chairman of the Federal Trade Commission, the secretary of Homeland Security, and the Attorney General.”).

112 See Rozenshtein, supra note 98 (laying out that the remaining 16 members “would include four representatives from law enforcement, four from the community of child-exploitation victims, two legal experts, two technology experts and four representatives from technology companies.”). See also Pfeferkorn, supra note 102 (explaining that other representatives from law enforcement would sit on the commission); Lily Hay Newman, The EARN IT Act is a Sneak Attack on Encryption, WIRED (Mar. 5, 2020), archived at https://perma.cc/W7MA-LXM3 (noting the commission would consist of 16 other members).

113 See Dahan, supra note 104 (explaining that the remaining members would be “selected by the leaders of the Senate and the House of Representatives.”). See also Rozenshtein, supra note 98 (noting that the other members were “to be chosen by the heads of each party in the House and Senate”).

114 See id. (stating that “support of 14 members would be required to approve any best practices.”).

115 See id. (explaining that “the Attorney General, along with the other two agency heads, must accept or reject the recommendations outright.”). It is important to note that this is a substantial change from the initial draft that circulated which stated that the “attorney general could modify the recommendations for any reason, rendering the commission merely advisory.” Id. In the first draft circulated to the Senate, the Attorney General could act alone without the approval of other agencies. Id.
Federal Register. Lastly, before the recommendation could go into practice, it would be have to be enacted by Congress.

B. “Manager’s Amendment”

On July 2, 2020, the Senate Judiciary Committee published a “manager’s amendment” from Senator Graham and Senator Blumenthal. The manager’s amendment reflected significant changes to the first draft of the bill. Most notably, the Amendment eliminated the provision making Section 230 immunity contingent upon compliance with the Act’s best practices. This significant change meant that companies could receive immunity regardless of their compliance with the best practices. The Amendment still

---

116 See Pfefferkorn, supra note 102 (stating that while the Attorney General no longer has power to approve or disapprove of the best practices, the Attorney General still has some influence and publishes the best practices to their websites).
117 See Rozenshtein, supra note 98 (noting that “before any recommendation goes into practice, Congress must enact it”). It is also important to note that this is again a change from the initial draft, which stated that “recommendations would enter into force unless Congress affirmatively rejected them.” Id. This change reflects that Congress receives the final approval on the recommended best practices for tech companies. Id.
118 See Pfefferkorn, supra note 102 (stating that “[o]n July 2, the Senate Judiciary Committee held a full committee hearing at which it made significant changes to the pending EARN IT Act Bill [. . .] Senator Lindsey Graham [. . .] introduced a [. . .] manager’s amendment”). See also Birnbaum, supra note 102 (explaining that the committee published a “manager’s amendment” in July); Derek B. Johnson, EARN IT Act Sails through Senate Judiciary Committee, FCW (July 6, 2020), archived at https://perma.cc/CGS9-DZLK (explaining that a modified version of the act was before the Senate Judiciary Committee in July).
119 See Pfefferkorn, supra note 102 (stating that Senate Judiciary Committee made “significant changes” to the bill at the Senate Judiciary hearing in July).
120 See Birnbaum, supra note 102 (explaining that under the manager’s amendment, the act would “no longer make Section 230 immunity conditional on compliance with government mandated ‘best practices’”). See also Dahan, supra note 104 (stating that after the amendment, “adherence to the ‘best practices’ is no longer compulsory”); Johnson, supra note 118 (explaining that the manager’s amendment stripped the DOG of legal authority to enforce their best practices); Hannah Quay-de la Vallee & Mana Azarmi, The New EARN IT Act Still Threatens Encryption and Child Exploitation Prosecutions, CTR. FOR DEMOCRACY AND TECH. (Aug. 25, 2020), archived at https://perma.cc/V9RZ-ZF4E (noting that under the amendments, “there is no longer any constructive way for companies to ‘earn’ the liability shield provided by Section 230”).
121 See Corinne Day, EARN IT Manager’s Amendment Welcome, But Needs Work, Says R Street Institute, RSTREET (July 2, 2020), archived at https://perma.cc/7WDT-
created a commission to determine best practices to be followed by tech companies; however, it made compliance voluntary.\textsuperscript{122} This change was significant as it eliminated some of the authority granted to the commission.\textsuperscript{123}

Additionally, the Amendment removed language that left companies at a higher risk for lawsuits.\textsuperscript{124} Under the initial draft, tech companies could be held federally liable for civil penalties if they “recklessly” provided a service that was used to disseminate child sexual abuse material.\textsuperscript{125} A reckless standard of liability means that the actor knew or should have known that their conduct would likely cause harm.\textsuperscript{126} Under the amended bill, the aforementioned language was removed, returning it to a “knowingly” liability standard.\textsuperscript{127} Under a knowledge standard, the actor must have direct and clear

\begin{itemize}
\item[85K9] (noting that the manager’s amendment makes “best practices [. . .] advisory rather than legally operative”).
\item[122] See Birnbaum, supra note 102 (explaining that under the amendment, the bill still creates a commission that determines “best practices” but that those recommendations are now “voluntary rather than legally required.”). The amendment would still change Section 230 to allow federal and state claims against companies, but it “would not empower the commission to make potentially unconstitutional demands of the companies.” Id.
\item[123] See Day, supra note 121 (explaining that the manager’s amendment removed some of the legal authority of the bill-created commission).
\item[124] See Birnbaum, supra note 102 (noting that the amendment would “remove a provision that would have left the companies vulnerable to significantly more lawsuits.”).
\item[125] See id. (explaining that prior to the amendment, the act called for the “reckless” standard to be applied to online platforms if they “provided a service that was used to distribute child sexual abuse material.”).

A person acts recklessly with respect to a material element of an offense when he consciously disregards a substantial and unjustifiable risk that the material element exists or will result from his conduct. The risk must be of such a nature and degree that, considering the nature and purpose of the actor’s conduct and the circumstances known to him, its disregard involves a gross deviation from the standard of conduct that a law-abiding person would observe in the actor’s situation.

Id.
\item[127] See Birnbaum, supra note 102 (noting that under the amendment, the “reckless “standard is removed, and the standard becomes “knowingly”).
\end{itemize}
knowledge that their conduct would cause harm. The Amendment also limited the scope of civil and criminal charges to be brought under state law, holding companies liable in state court “regarding the advertisement, promotion, presentation, distribution, or solicitation of child sexual abuse material.”

Additionally, The Senate Judiciary Committee adopted an amendment from Democratic Vermont Senator Patrick Leahy in July 2020. This Amendment clarified that tech companies who provided end-to-end encryption services could not be subject to liability under the Act. Under the Amendment, tech companies are not liable if they do not possess the information to decrypt the communication. Additionally, technology companies are not liable if they fail to take


A person acts purposely with respect to a material element of an offense when: (i) if the element involves the nature of his conduct or a result thereof, it is his conscious object to engage in conduct of that nature or to cause such a result; and (ii) if the element involves the attendant circumstances, he is aware of the existence of such circumstances or he believes or hopes that they exist.

Id.

129 See Pfefferkorn, supra note 102 (noting that the manager’s amendment changes the scope of state-law criminal and civil charges against providers). Under the amendment, state criminal and civil actions can be brought against providers for state-law equivalents of certain subsections of federal laws “regarding the advertisement, promotion, presentation, distribution, or solicitation of child sexual abuse material.” Id. See also Johnson, supra note 118 (explaining that the amendment revoked Section 230 protections for state laws and federal civil claims).

130 See Quay-de la Valle & Azarmi, supra note 120 (explaining Senator Leahy introduced and secured his own amendment to the act). See also Makena Kelly, A weakened version of the EARN IT Act advances out of committee, THE VERGE (July 2, 2020), archived at https://perma.cc/2EBG-NTT2 (noting that Leahy filed for his own amendment which was approved and incorporated into the bill that will go to the floor for a vote).

131 See Dennis Fisher, House Version of The EARN IT ACT Introduced, DECIPHER (Oct. 2, 2020), archived at https://perma.cc/5RMH-KKQQ (explaining that the Leahy amendment “says that platform providers could not be held liable for offering encrypted services or not having the ability to decrypt users’ communications.”). See also Pfefferkorn, supra note 102 (explaining that “Leahy’s amendment tries to create an encryption safe harbor.”); Quay-de la Vallee & Azarmi, supra note 120 (explaining that Leahy’s amendment “seeks to prevent EARN IT from precluding a provider from offering encrypted services.”).

132 See Pfefferkorn, supra note 102 (explaining that the Leahy amendment “speaks out that a provider may not be held liable because it . . . ‘does not possess the information necessary to decrypt a communication’ . . . ”).
action that would undermine the ability of the provider to offer encrypted services.  

The July 2020 Amendment reflected the same changes from the Manager’s Amendment. While the AG remains head of the commission, the power of the office is limited, as the AG’s powers were rolled back. Under the amended draft, the AG does not have power to approve or disapprove the best practices. Instead, the AG publishes the best practices on the DOJ Website and the Federal Register. On July 2, 2020, the Senate Judiciary Committee voted to approve the EARN IT Act unanimously. The legislation waits to be considered by the Senate. In the meantime, a nearly identical bill was introduced to the House of Representatives.

133 See id. (noting that “provider[s] may not be held liable because [they] ‘utilize[] full end-to-end encrypted messaging services, device encryption, or other encryption services’; ‘does not possess the information necessary to decrypt a communication’; or ‘fails to take an action that would otherwise undermine the ability of the provider to offer full end-to-end encrypted messaging services, device encryption, or other encryption services.’”). See also Fisher, supra note 131 (explaining that the Leahy amendment contains explicit reference to encrypted services and devices and that companies are not liable if they do not have the ability to decrypt communications).

134 Compare Pfefferkorn, supra note 102 (acknowledging that the Attorney General’s power is more limited under the July amendment), with Rozenshtein, supra note 98 (explaining that under the March amendments, the Attorney General’s power had been limited).

135 See Pfefferkorn, supra note 102 (explaining that the manager’s amendment “removes some of the Attorney General’s formerly broad power over the best practices.”).

136 See id. (noting that the Attorney General “no longer has the power to prove or disapprove the commission’s best practices.”).

137 See id. (explaining that in the manager’s amendment, “the AG instead just has to publish the best practices on the Department of Justice’s website and in the Federal Register.”)

138 See Johnson, supra note 118 (explaining that the modified version of the EARN IT Act was unanimously passed by the Senate Judiciary Committee in July).

139 See id. (explaining that after being passed by the Senate Judiciary Committee in July, the bill sets up a “high-stakes floor vote . . .”). See also Kelly, supra note 130 (noting that the act awaits a vote on the floor).

140 See Fisher, supra note 131 (noting that the House version of the act was introduced in September). See also Caleb Chen, Representatives Garcia and Wagner introduce EARN IT Act to the House, PRIV. NEWS ONLINE (Oct. 5, 2020), archived at https://perma.cc/5T67-LN43 (explaining that the act had been submitted to the House of Representatives).
C. Bill Introduced to the House

On September 30, 2020 a similar EARN IT Act was introduced in the House of Representatives.\(^{141}\) The bill was introduced in the House with bipartisan support from Democratic Representative Sylvia Garcia and Republican Representative Ann Wagner.\(^{142}\) The House Bill has the same goal as the Senate Bill: to slow the spread of CSAM and hold tech companies responsible for monitoring content.\(^{143}\) The House Bill also creates a commission to establish best practices companies would be encouraged to follow for immunity under Section 230.\(^{144}\)

There is, however, at least one notable difference between the House Bill and the Senate Bill.\(^{145}\) The House Bill adds that full end-to-end encrypted messaging services, device encryption, and other encryption devices cannot be used as the sole basis for liability.\(^{146}\) This

\(^{141}\) See Fisher, \textit{supra} note 131 (explaining that the House version “includes virtually all of the same language as the Senate Bill.”)

\(^{142}\) See \textit{Representatives Sylvia Garcia and Ann Wagner Introduce the Bipartisan EARN IT Act in the House of Representatives, CONGRESSWOMAN SYLVIA GARCIA: REPRESENTING THE 29TH DIST. OF TEXAS} (Sept. 30, 2020), \textit{archived at} https://perma.cc/ZGL6-Z9XH (noting the two representatives who introduced the legislation and that it was a bipartisan effort, like its counterpart in the Senate).

\(^{143}\) See Fisher, \textit{supra} note 131 (explaining that the bill, like the Senate bill, is “intended to curb the spread of child exploitation material by placing some new responsibilities on platform providers to identify and report such material.”).

\(^{144}\) See \textit{id.} (explaining the similarities between the House bill and the Senate bill, including for the commission to establish best practices). \textit{See also} Chen, \textit{supra} note 140 (explaining that the act would create a commission “that will be responsible for drafting a set of rules that internet companies must follow in order to continue being eligible for protections under Section 230 of the CDA . . . .”).

\(^{145}\) See Fisher, \textit{supra} note 131 (explaining that the “House bill has similar language, with one significant change”). \textit{See also} Muralidharan Palanisamy, \textit{EARN IT Act and How Encryption is Related to Freedom of Speech, SEC. BOULEVARD} (Nov. 27, 2020), \textit{archived at} https://perma.cc/E8YQ-FKHA (noting that the amended version introduces a few significant changes to the original version).

\(^{146}\) See Fisher, \textit{supra} note 131 (stating that the change in the House bill notes that encryption cannot be used as the sole basis for liability). The factors that cannot be used as the sole basis for liability in the House bill are as follows:

- The provider utilizes full end-to-end encrypted messaging services, device encryption, or other encryption services. The provider does not possess the information necessary to decrypt a communication. The provider fails to take an action that would otherwise undermine the ability of the provider to offer full end-to-end encrypted messaging services, device encryption, or other encryption services.
differs from the Senate Bill, which provides shelter for encryption.147 Essentially, the language in the House Bill allows for encryption services to be used as evidence for liability, just not the only evidence.148

IV. Analysis

A. Threat to Public Safety

Special Agent Flint Waters testified before Congress in 2007 explaining the horrors that he witnessed while investigating child sexual abuse.149 He described the problem as a “tidal wave of tragedy” and law enforcement as “drowning.”150 It is clear that the proliferation of CSAM online is a dire problem.151 In drafting

Id.

147 See id. (explaining that the Leahy amendment, which provides cover for encrypted services, is not included in the House version).

148 See id. (explaining that encryption is able to be used as a factor for a company’s liability, just not the only factor).

149 See Keller & Dance, supra note 1 (explaining that Special Agent Flint Waters worked as a criminal investigator in Wyoming and testified before Congress in 2007 about his work). See also Sweigart, supra note 37 (reporting that experts have seen an increase in both quantity and extremity of child sexual abuse online); Child Sexual Abuse Material (CSAM), supra note 2 (describing CSAM as a “disturbing reality”). While girls are in the majority of these materials, when boys are victimized, they are more likely to be subjected to “explicit or egregious abuse.” Child Sexual Abuse Material (CSAM), supra note 2. See also Encryption trend threatens child safety gain, supra note 3 (explaining that with every share of CSAM online, there is a cycle of revictimization for the survivor).

150 See Keller & Dance, supra note 1 (quoting Special Agent Waters as saying, “[w]e are overwhelmed, we are underfunded, and we are drowning in the tidal wave of tragedy.”). See also Salter, supra note 3 (explaining that “[o]ver the last decade, reports of CSAM to US authorities have been increasing by 50% per year”); Breland, supra note 37 (noting that “[l]aw enforcement agencies assigned to tackle the problem say they are understaffed and underfunded”); Sweigart, supra note 37 (reporting that Ohio law enforcement agencies have concerns about the rising reports of CSAM and the lack of resources available to them to combat the problem). While reports of CSAM have increased dramatically, the national arrest numbers for abusers have stayed relatively flat, which lawmakers attribute to a lack of resources for the agencies on the front lines. Sweigart, supra note 37.

151 See Jerome, supra note 1 (citing data that shows child sexual abuse material and crimes are steadily increasing). See also Keller & Dance, supra note 1 (explaining that tech companies reported a record number of reports of CSAM in 2018); Slater, supra note 1 (referencing 2019 reports that included 69.1 million forms of child
legislation, however, Congress struggles to balance individual freedoms with public safety.\textsuperscript{152}

Based on the drafts of the EARN IT Act, activists are concerned that the Act threatens Fourth Amendment rights.\textsuperscript{153} Though the Act has evolved over time, what “best practices” will entail remains unclear.\textsuperscript{154} While Section 230 immunity no longer hinges upon best practice compliance, companies are encouraged to voluntarily comply.\textsuperscript{155} It seems futile to make the best practices voluntarily because if companies are actually incentivized to adhere to the practices, it is more likely they will comply.\textsuperscript{156} One concern voiced

sexual exploitation); Butler, \textit{supra} note 28 (noting that “[o]nline child sexual exploitation has skyrocketed during the coronavirus pandemic”); Racioppi, \textit{supra} note 28 (explaining that efforts by both the government and technology companies to deal with the distribution of CSAM are “welcome and long overdue.”); \textit{Encryption trend threatens child safety gains, supra} note 3 (referring to the trading of CSAM as “a well-documented crisis.”).

\textsuperscript{152} See \textit{CDA 230: The Most Important Law Protecting Internet Speech, supra} note 75 (discussing the importance of Section 230 of the Communications Decency Act in protecting individual liberties such as freedom of speech and expression on the internet). \textit{See also} Salter, \textit{supra} note 3 (emphasizing that “[t]he technology industry has been vocal in denouncing online child sexual exploitation however they have often been unwilling to prioritize child protection over their business prerogatives.”). \textit{But see Rodrigo, supra} note 72 (explaining how many legislators see Section 230 as a hindrance to holding tech companies liable for criminal activity facilitated by their platforms); \textit{Encryption trend threatens child safety gains, supra} note 3 (commending Google for “demonstrat[ing] that a balance between privacy and child protection is possible.”).

\textsuperscript{153} See \textit{U.S. Const. amend. IV} (asserting the right Americans have to be protected against unreasonable searches and seizures). \textit{See also} Karr, \textit{supra} note 8 (explaining that when the bill was introduced in Congress, it was heavily criticized by free-speech and digital-rights groups); Birnbaum, \textit{supra} note 102 (noting that critics are concerned about the threats to the Fourth Amendment that the EARN It Act could hold).

\textsuperscript{154} See Karr, \textit{supra} note 8 (quoting a statement made by a Free Press Action Senior Policy Council member who explained that the public does not yet know what the best practices might look like but that ideas currently exist based on the DOJ’s own floating of proposed best practices). \textit{See also} Rozenshtein, \textit{supra} note 98 (describing the best practices as “to-be-determined.”).

\textsuperscript{155} See Birnbaum, \textit{supra} note 102 (explaining that the bill still creates a commission that creates “best practices” but that those recommendations are “voluntary rather than legally required.”). \textit{See also} Day, \textit{supra} note 121 (stating that the manager’s amendment made the best practices recommended by the commission advisory rather than “legally operative”).

\textsuperscript{156} See Baker, \textit{supra} note 106 (explaining that companies are “free to ignore the recommendations of the commission and the [AG], . . . and they will still have two
among experts is that “best practices” will encourage companies to be more proactive in monitoring their users content and in reporting them to law enforcement.\textsuperscript{157} While this is a legitimate concern, given the enormity of the CSAM problem, it is unlikely companies will have the capacity to monitor unrelated communications.\textsuperscript{158}

### B. Search and Seizure

#### 1. Protected Interest

In determining whether Fourth Amendment protections apply to tech companies’ surveillance of online communications, it must be determined whether there is a legitimate expectation of privacy.\textsuperscript{159} The ways to avoid liability.”). \ See also Quay-de la Vallee & Azarmi, \textit{supra} note 120 (explaining that under the amendment, tech companies do not have a clear way to earn their liability and prevent CSAM).\textsuperscript{157} \ See Pfefferkorn, \textit{supra} note 102 (explaining that the act has a “‘state actor’ problem” and that while the best practices are now explicitly voluntary, there is still a question of whether tech companies will be considered state actors in closely monitoring users’ communications for child sexual abuse material). Additionally, the drafters of the act anticipated push back on this issue and issued a disclaimer saying that nothing in the bill required technology companies “to search, screen, or scan” for CSAM. \textit{Id}. \ See also Birnbaum, \textit{supra} note 102 (noting that critics of the act “claimed the commission’s recommendations could violate the Fourth Amendment if they required companies to search for particular kinds of content.”). \textsuperscript{158} \ See Slater, \textit{supra} note 1 (noting that in 2019, reports to the National Center for Missing and Exploited Children’s CyberTipline included 69.1 million forms of child sexual exploitation). \ See also Keller & Dance, \textit{supra} note 1 (explaining that in 2019, “tech companies reported a record 45 million online photos and videos of . . . [abuse]”); \textit{Encryption trend threatens child safety gains, supra} note 3 (reporting that in 2019, the reports of CSAM to authorities represented over 15,000% growth in reports over the previous 15 years). Additionally, these numbers only reflect instances of CSAM that have been reported to authorities and it is known that there is much more that has remained undetected or reported. \textit{Encryption trend threatens child safety gains, supra} note 3. \textsuperscript{159} \ See U.S. CONST. amend. IV (enumerating the categories of items which the protections apply to, including “persons, houses, papers, and effects”). \ See also \textit{History and Scope of the Amendment, supra} note 85 (explaining what interests are protected under the Fourth Amendment and the significance of the \textit{Katz} decision in defining what is protected under the Fourth Amendment); Katz v. United States, 389 U.S. 347, 351 (1967) (holding where there was a reasonable expectation of privacy). \textit{But see United States v. Miller, 425 U.S. 435, 446 (1976)} (holding that there is no protected privacy interest in bank records); Smith v. Maryland, 442 U.S. 735, 745 (1979) (holding that there is no protected privacy interest in phone numbers dialed);
Supreme Court has held that this protection does not include information a person knowingly exposes to the public.\textsuperscript{160} In contrast, what an individual seeks to preserve as private, even if accessible to the public, is protected.\textsuperscript{161} Following the decision in Katz, if an individual intends to keep their online communications private, then that communication should be protected under the Fourth Amendment.\textsuperscript{162} It must be considered whether there is a reasonable expectation of privacy in information provided to a third party such as a social media site.\textsuperscript{163}

California v. Greenwood, 486 U.S. 35, 45 (1988) (holding that there is no right to privacy in what one presents to a third party).
\textsuperscript{160} See Katz, 389 U.S. at 351 (holding that what a person knowingly exposes is not protected by the Fourth Amendment). See also Maclin, supra note 83, at 55 (noting that Katz was a landmark case that redefined the scope of the Amendment and solidified that the Constitution required judicial supervision of electronic surveillance); Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (explaining that “[w]hen an individual ‘seeks to preserve something as private’ and his expectation of privacy is ‘one that society is prepared to recognize as reasonable,’ we have held that official intrusion into that sphere generally qualifies as a search and requires a warrant supported by probable cause.”).
\textsuperscript{161} See History and Scope of the Amendment, supra note 85 (noting that the holding in Katz explained what is and is not protected under the Fourth Amendment is what one knowingly exposes to the public and seeks to keep private). See also Katz, 389 U.S. at 350–51 (holding that what a person intends to keep as private is afforded protection under the Fourth Amendment); Kyllo v. United States, 533 U.S. 27, 40 (2001) (explaining that methods that expose what a person intends to keep private that could not otherwise be obtained without a physical invasion are in violation of the Fourth Amendment).
\textsuperscript{162} See Katz, 389 U.S. at 350 (holding that what a person knowingly exposes is not protected by the Fourth Amendment, and what a person intends to keep as private, even if accessible to the public, still falls under the protections afforded in the Amendment). See also Carpenter, 138 S. Ct. at 2214 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)) (noting that basic guideposts of Fourth Amendment protections under case law include securing “the privacies of life” against “arbitrary power” and “to place obstacles in the way of a too permeating police surveillance.”).
\textsuperscript{163} See Miller, 425 U.S. at 436–37 (holding that there is no Fourth Amendment interest in bank records); Smith, 442 U.S. at 745 (holding that there is no Fourth Amendment privacy in phone numbers dialed); Greenwood, 486 U.S. at 41 (holding that there is no Fourth Amendment protection in something one gives to a third party or that is readily observable by police). See also Mund, supra note 97, at 244 (explaining that “courts have found the third-party doctrine dispositive” in determining the privacy interests associated with social media communications). “If the third-party doctrine governs social media behavior, then published content voluntarily shared among connections within a private social network loses all reasonable expectation of privacy, including any reasonable expectation that a user’s
Communications that take place over social media platforms are generally not afforded Fourth Amendment protections. Law enforcement is not required to obtain a warrant to search these records and can collect relevant evidence with a subpoena. Other information, such as communications shared publicly with Facebook friends, do not require a request. Law enforcement may even create fake profiles to investigate and monitor potential suspects accounts. While this may seem underhanded, it follows the traditional logic of *Katz*, *Smith*, and *Miller*—information an individual knowingly exposes connections will not turn over their social data to investigative authorities.” *Id.* at 244–45.

164 See Fassler, *supra* note 80 (noting that Facebook data is accessible by government-issued subpoenas and that it is “relatively easy for law enforcement to make such requests.”). Facebook even offers law enforcement a portal to simplify the process of making a data request. *Id.* See also Mund, *supra* note 97, at 244 (remarking that “government agents can presumably gain access to posted social media data without meeting any probable cause requirements.”). Essentially, the publisher of a social media communication is aware that any content is recorded on the website’s platform, and the publisher takes a risk that a social media connection may repeat what they have seen. *Id.* at 249.

165 See Fassler, *supra* note 80 (explaining that law enforcement can obtain data from Facebook by sending a search warrant or a government-issued subpoena for data). Additionally, Facebook voluntarily hands over data in response to “emergency requests” from law enforcement where a case involves death or potential bodily harm. *Id.* In 2019, 6,447 emergency requests were made to Facebook from law enforcement agencies. *Id.*

166 See TheBestVPN LTD., *supra* note 80 (explaining “every time someone posts information publicly, either on their personal page or in public groups, that information can legally be used in criminal investigations” with no need for a subpoena to access that information). See also Mund, *supra* note 97, at 248 (explaining that courts have compared public social media posts “to screaming the content out of an open window, and that sharing information on the internet is akin to sharing information in the middle of a public street.”). Even if users post to a closed social network, courts have still ruled that “publishers lose all reasonable expectation of privacy to that data.” *Id.*

167 See TheBestVPN LTD., *supra* note 80 (describing how in serious cases, law enforcement has used an undercover profile to add suspects as friends in order to get access to their information). See also Mund, *supra* note 97, at 252 (explaining how the government “may also attempt to access social networking data more directly – by creating an account and asking an individual to permit entry into their social network.”). “[I]f an individual accepts a friend request from an undercover government agent, that acceptance provides the same access as if the individual knowingly exposed permitted their private social media publications to the government agent.” *Id.* at 252–53.
to the public or gives to a third party is not protected. As a result, these tactics are fair for law enforcement to use in an investigation.

Given the ever-evolving nature of technology, the idea of privacy in social media communications is changing. Case law surrounding technology and Fourth Amendment protections are slow to reflect new technologies, including cell phones. In Riley v. California, the Supreme Court held that a warrantless search of the digital contents of a cell phone seized incident to an arrest was unconstitutional. More recently, the Supreme court held in Carpenter that CSLI was considered protected information given its

---

168 See Miller, 425 U.S. at 446 (holding that bank records are not protected by the Fourth Amendment under the third-party doctrine). See also Smith, 442 U.S. at 745 (holding there was no reasonable expectation of privacy in the number dialed under the third-party doctrine).

169 See Malan, supra note 27 (explaining that the extraordinarily fast technological and social changes that have occurred in the Fourth Industrial Revolution have made it difficult to rely only on government legislation because the legislation is likely to be out-of-date or redundant by the time it is implemented). See also Maclin, supra note 83, at 52 (remarking how “[w]ith the increased use of technology in the twentieth century, the Supreme Court confronted search and seizure questions never imagined by the Framers.”).

170 See Ferguson, supra note 84, at 806 (explaining that new technologies, such as interactive devices, have created problems for the interpretation of the protection of “persons, houses, papers, and effects” from unreasonable searches and seizures by the government). See also Mund, supra note 97, at 244 (noting that courts have not yet reached a “content versus non-content distinction when assessing social media communications.”). Courts have reached this distinction regarding items like letters and packages. Id. Mailed letters and sealed packages are protected from examination and inspection, other than their outward appearance. Id. “Opening the envelope and searching its contents would violate the Fourth Amendment.” Id. See generally Riley v. California, 573 U.S. 373, 401 (2014) (holding that a physical cell phone can be seized incident to arrest, but that its digital contents require a warrant to be searched); Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (holding that cell site location information is protected under the Fourth Amendment and requires a warrant to obtain); Agosta, supra note 90, at 131 (explaining that before the Supreme Court ruled on the constitutionality of certain aspects of cell phone data, “individuals [were] at risk of having their most personal information viewed by an arresting police officer, no matter how minor the arrest may be.”).

171 See Riley, 573 U.S. at 395–96 (holding that data stored on a cell phone is distinguishable from a physical record and comprehensive in revealing the specific movements of a cell phone owner and the data would reveal far more about a person’s life than a physical search of a home). See also Yelton, supra note 88, at 998 (explaining “the Court acknowledged that digital and physical materials are different and should be analyzed accordingly.”). “But the Court refused to classify a cell phone as a container, analogizing the relationship of physical objects and data to a ride on horseback and a trip to the moon.” Id. at 1028–29.
“unique nature” of storing information regarding how and when a person travels in a retrospective and all-encompassing manner. These decisions carry Fourth Amendment implications regarding social media. Currently, the law does not require law enforcement to obtain a warrant to search users’ social media communications. Under the third-party doctrine these communications are not protected, however, this could change given the presence of social media.

2. Government Action

The next question whether tech companies searching users’ private communications constitutes government action. Whether a

---

172 See Carpenter, 138 S. Ct. at 2220 (holding that CSLI was protected under the Fourth Amendment due to its “deeply revealing nature . . . depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection”). See also Thomas, supra note 88, at 2224 (explaining the holding in Carpenter signaled “that a person maintained an expectation of privacy society was willing to recognize even after they shared that information with a third party.”). See Social Media Fact Sheet, supra note 90 (noting that in 2005, only 5% of American adults used a social media platform, which significantly rose to 72% of American adults by 2019). See also Mund, supra note 97, at 239 (explaining “[e]veryday conversations amongst friends – the sort that traditionally constituted private speech – now transpire over social platforms like Facebook, Twitter, and LinkedIn.”). “With users of social networking sites increasingly sharing their life experiences online, social platforms may contain an extensive record of information documenting an individual’s activities, preferences, and opinions.” Id.

173 See Fassler, supra note 80 (noting that social media data is easily obtained by law enforcement through subpoenas or Facebook’s law enforcement portal). See also Mund, supra note 97, at 244 (explaining that government agents can obtain social media communications without establishing probable cause); TheBestVPN LTD., supra note 80 (explaining that information a user posts publicly, on a personal page, or in a social media group can be obtained by law enforcement without even a subpoena).

174 See Carpenter, 138 S. Ct. at 2223 (holding that CSLI was protected under the Fourth Amendment due to how intimate and comprehensive its data was). See also Mund, supra note 97, at 239 (noting that social media users have a "misguided sense of security that information shared within personal networks will remain private."). Social media sites now routinely capture a thorough record of an individual’s “activities, preferences, and opinions.” Id.

175 See Pfefferkorn, supra note 102 (explaining that while changes have been made to make the best practices voluntary, it creates a problem for tech companies in which they are forced to choose between following the best practices or not and the consequences of that choice). See also Birnbaum, supra note 102 (explaining the
private party is considered an agent of the government depends on the extent that the government participated in the private parties’ activities and is fact determinative.\textsuperscript{177} A court considers three factors to determine whether a private party acts as an agent of the government including: whether the government had knowledge of the conduct; whether the citizen intended to assist law enforcement; and whether the citizen acted at the request of the government.\textsuperscript{178} In this case, the government is directing the tech companies to comply with best practices and officials clearly would have knowledge of the tech companies’ searching communications.\textsuperscript{179}

Based on precedent set in United States v. Smith, a court must then look to the intent of the actor in aiding law enforcement to determine whether the actor is an agent of law enforcement.\textsuperscript{180} In Smith, the court held that where the actor was not motivated solely or primarily by the intent to aid law enforcement, they are not considered an agent.\textsuperscript{181} These facts are not significantly different from the potential best practices of the EARN IT Act, where tech companies may be searching users’ communications for the purpose of aiding law

\textsuperscript{177} See United States v. Smith, 383 F.3d 700, 705 (2004) (noting that searches by private citizens are not restricted by the Fourth Amendment in the same was that searches by government agents are). Additionally, several factors are considered when determining whether private citizens were acting as government agents. \textit{Id.}

\textsuperscript{178} See \textit{id.} (explaining the test).

[Whether] the government had knowledge of and acquiesced in the intrusive conduct; whether the citizen intended to assist law enforcement agents or instead acted to further his own purposes; and whether the citizen intended to assist law enforcement agents or instead acted to further his own purposes, and whether the citizen acted at the government’s request.

\textit{Id.}

\textsuperscript{179} See \textit{Introduce EARN IT Act}, \textit{supra} note 6 (explaining how the act would create a commission that would recommend best practices to tech companies regarding how to monitor CSAM on their platforms). \textit{See also} Rozenshtein, \textit{supra} note 98 (noting that the act would set up a commission “to develop best practices that companies would have to adopt to get immunity”); Birnbaum, \textit{supra} note 102 (explaining the commission created by the bill still recommends best practices, but the best practice compliance is voluntary).

\textsuperscript{180} See \textit{Smith}, 383 F.3d at 705 (holding that the private actor was motivated by employer obligations and, in part, to aid law enforcement).

\textsuperscript{181} See \textit{id.} (holding that where a private actor is “motivated in part by a desire to aid law enforcement does not in and of itself transform her into a government agent.”).
Tech companies would be motivated to help law enforcement catch illegal material on their platforms but also to earn their Section 230 immunity. Where a court sees that an actor has a dual motive for their actions, the actor may not necessarily be considered an agent of law enforcement. In United States v. Highbull, the court determined where an actor had a dual motive of aiding law enforcement and protecting their child, the actor was not considered an agent of law enforcement. In this case, tech companies may argue that they are not solely acting on behalf of the government in searching users’ communications for CSAM. The companies may argue that they have an interest in maintaining the integrity of their site and the safety of their users by monitoring communications for illegal activity, as

---

182 See id. (holding that the actor in Smith was partly motivated by a desire to aid law enforcement and partly motivated by requirements of the actor’s job). But see Dahan, supra note 104 (explaining that the best practices would be developed and directed to tech companies by the government commission for best practices that would include law enforcement members).

183 See Introduce EARN IT Act, supra note 6 (explaining how the act was created to encourage tech companies to work with law enforcement in order to combat the issue of child sexual exploitation). See also Smith, 383 F.3d at 705 (holding that private citizens become government agents where they are motivated “solely or even primarily” by the intent to aid law enforcement).

184 See United States v. Highbull, 894 F.3d 988, 993 (2018) (holding that the actor was not acting as a government agent where there was no evidence that the actor was motivated primarily by a desire to help the police). See also United States v. Benoit, 713 F.3d 1, 10 (2013) (holding that the private citizen had a “legitimate, independent motivation” to conduct a search of the defendant outside of helping law enforcement); United States v. Harling, 705 F. App’x 911, 916 (2017) (holding that the two private citizens in question “acted of their own accord” when they conducted a search of the defendant’s USB drive).

185 See Highbull, 894 F.3d at 993 (holding that the actor was motivated not to primarily help police, but rather to protect her daughter from a potential predator). See also Benoit, 713 F.3d at 10 (holding that the private citizen had a “legitimate, independent motivation” to conduct a search of the defendant outside of helping law enforcement); Harling, 705 F. App’x at 916 (holding that the two private citizens in question “acted of their own accord” when they conducted a search of the defendant’s USB drive).

186 See Highbull, 894 F.3d at 993 (finding that the actor was “animated at least as much by a compulsion to protect her daughter as she was by any desire to aid the police”). See also Smith, 383 F.3d at 705 (holding that where a private actor is in part “motivated by a desire to aid law enforcement does not in and of itself transform her into a government agent.”).
well as earning their immunity.\textsuperscript{187} If this argument is successful, tech companies may not necessarily be considered government agents.\textsuperscript{188}

Lastly, in this case the government is directing tech companies to perform searches through best practices.\textsuperscript{189} Although the companies may argue they were not solely acting to help law enforcement, there is potential they could be seen as government actions.\textsuperscript{190} Proliferation of CSAM, however, is not a problem that will be disappearing anytime soon.\textsuperscript{191} Given the magnitude of the problem, it is unlikely that tech companies have the capacity to search and report unrelated activities.\textsuperscript{192} Additionally, society must reflect on how much privacy one really possesses in social media communications.\textsuperscript{193}

\textsuperscript{187} See Highbull, 894 F.3d at 993 (holding that where there are dual motives for a private citizen conducting a search and the non-governmental motive is the primary reason, a private citizen may not be considered an agent of the government).

\textsuperscript{188} See id. (noting that where the primary motivation of the citizen was to protect her child, the actor was not considered an agent of law enforcement). See also Benoit, 713 F.3d at 10 (holding that the private citizen had a “legitimate, independent motivation” and therefore was not considered a government agent); Harling, 705 F. App’x at 916 (holding that the two private citizens in question had an independent motive for conducting their search and were considered independent sources rather than government agents).

\textsuperscript{189} See \textit{Introduce EARN IT Act}, supra note 6 (explaining how the act would create a commission that would recommend best practices to tech companies regarding how to monitor CSAM on their platforms).

\textsuperscript{190} See Highbull, 894 F.3d at 993 (holding that a person may be considered a government agent where they are acting with the primary intent of aiding law enforcement). See also Smith, 383 F.3d at 705–06 (holding that a private citizen may become a government agent where the private citizen is motivated “solely or even primarily” by the intent to aid law enforcement).

\textsuperscript{191} See Keller & Dance, supra note 1 (stating that tech companies reported a record 45 million online photos and videos of child sexual abuse in 2018). See also Jerome, supra note 1 (explaining how recent research suggests that child sexual abuse material and crimes are steadily increasing); Slater, supra note 1 (noting that in 2019, reports to the National Center for Missing and Exploited Children’s CyberTipline included 69.1 million forms of child sexual exploitation).

\textsuperscript{192} See Keller & Dance, supra note 1 (explaining that law enforcement is already overworked and underfunded to deal with a fraction of CSAM cases). See also Salter, supra note 3 (explaining that “[o]ver the last decade, reports of CSAM to US authorities have been increasing by 50% per year”); Breland, supra note 37 (noting that “[l]aw enforcement agencies assigned to tackle the problem say they are understaffed and underfunded”); Sweigart, supra note 37 (reporting that Ohio law enforcement agencies have concerns about the rising reports of CSAM and the lack of resources available to them to combat the problem).

\textsuperscript{193} See \textit{Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance}, supra note 80, at 1725 (explaining the role of tech companies in recent times as a liaison to law enforcement).
3. Special Needs Search

Proposed searches of social media communications under the EARN IT Act could fall under the umbrella of “special needs searches.” Special needs searches occur when there is a real, vital problem that can only be addressed effectively without a warrant because there is a need beyond normal law enforcement purposes that would be jeopardized if individual suspicion were required. The subjects of special needs searches traditionally fall under certain categories including government employees and agents, students, recipients of welfare, prisoners, and parolees. EARN IT Act searches would address a special kind of problem that may be compromised if individual suspicion were required - child sexual

194 See History and Scope of the Amendment, supra note 85 (explaining that in some cases no warrant, probable cause, or individualized suspicion is necessary for certain kinds of searches). See also Skinner v. Labor Exec. Ass’n, 489 U.S. 602, 655 (1989) (holding that this type of search was applicable where the probable cause and warrant requirements were not practicable to achieve the goal); Nat’l Treasury Emps. Union v. Von Raab, 816 F.2d 170, 179 (1987) (holding that the government had a compelling interest in determining that employees were not involved in the consumption of illegal drugs and that the search did not require individualized suspicion).

195 See History and Scope of the Amendment, supra note 85 (explaining cases where the court found there was a compelling government interest in conducting these searches without any individualized suspicion). See also Skinner, 489 U.S. at 625 (holding that the probable cause and warrant requirements were not practicable to achieve the goal of the search in question); Von Raab, 816 F.2d at 182 (holding that the search in question did not require individualized suspicion).

196 See History and Scope of the Amendment, supra note 85 (noting cases involving railroad employees, government employees, students, and other populations as falling within the special needs categories of searches). See also Skinner, 489 U.S. at 624 (holding that searches of train conductors were appropriate to prevent trains being driven by employees under the influence of drugs or alcohol); Von Raab, 816 F.2d at 178 (holding that drug testing programs for government employees who carry firearms, are involved in intercepting drug importation, or are in high level positions involving classified information are justified in departing from ordinary warrant and probable cause requirement by the substantial government interest in stifling the drug trade); Board of Ed. v. Earls, 536 U.S. 822, 837 (2002) (holding that drug testing students who wanted to participate in extracurricular activities was valid because students had limited privacy interests at school and the intrusion was minimal compared to the school’s interest in combating the drug problem).
abuse online. Given the serious nature of this crime, coupled with the fact that monitoring for these materials goes beyond normal law enforcement activities, this kind of search could fall under the category of a special needs search.

Searches called for by the EARN IT Act could fall under special needs searches for many of the same reasons that car checkpoints do. For example, in Michigan Department of State Police v. Sitz, the Supreme Court held that the gravity of drunk driving problems coupled with the magnitude of the state’s interest in getting drunk drivers off the road rendered a car check point constitutional. Additionally, because all of the cars were stopped in this check point it was better than targeting specific cars. Following the logic of Sitz,

197 See Introduce EARN IT Act, supra note 6 (explaining how the act came about to combat a particular problem in society regarding the circulation of CSAM online). See also Browne, supra note 57 (explaining how technological changes have made child sexual abuse online more sophisticated).

198 See History and Scope of the Amendment, supra note 85 (explaining cases that have demonstrated these types of searches require a compelling government interest and must go beyond the traditional scope of law enforcement to fall into this particular category). See also Skinner, 489 U.S. at 624 (holding that this type of search was applicable where the probable cause and warrant requirements were not practicable to achieve the goal); Mich. Dep’t of State Police v. Sitz, 496 U.S. 444, 454 (1990) (holding that the car check points were constitutional given the state’s interest in preventing drunk driving); Earls, 536 U.S. at 822 (holding that drug testing students correlated with the school’s strong interest in combatting the drug problem); Von Raab, 816 F.2d at 170 (holding that the government had a compelling interest in determining that employees were not involved in the consumption of illegal drugs and that the search did not require individualized suspicion).

199 See Sitz, 496 U.S. at 454 (holding that car checkpoints were constitutional absent a warrant where there was a compelling government interest and the manner in which citizens were searched was supported as effective by empirical data). See also English, supra note 82, at 454 (explaining how law enforcement agencies can “implement policies that will persuade individuals prone to drinking and driving” in this condition will very likely result in apprehension and punishment).

200 See Sitz, 496 U.S. at 455 (holding that the car check points were constitutional given the state’s interest in preventing drunk driving, how effective this system is in advancing that interest, and the minimal degree of intrusion upon the individual drivers). See also Earls, 536 U.S. at 822 (holding that drug testing students who wanted to participate in extracurricular activities was valid because students had limited privacy interests at school and the intrusion was minimal compared to the school’s interest in combatting the drug problem).

201 See Sitz, 496 U.S. at 454 (emphasizing that because this case does not conduct random stops, combined with empirical evidence, the stop is constitutional). See also English, supra note 82, at 460 (explaining that the difference between random checkpoints and the checkpoint in Sitz is that all cars that approached the checkpoint were stopped in Sitz).
data supporting the efficacy of preventing circulation of CSAM through monitoring all communications rather than targeting specific communications may support the constitutionality of the effort.\textsuperscript{202} Analogously, searches that result from the EARN IT Act are driven by the serious and prolific problem of child sexual abuse and the state has a strong interest in curtailing this problem.\textsuperscript{203} This, coupled with a search of all communications would potentially render the search constitutional under the \textit{Sitz} logic.

\section*{V. Conclusion}

Child sexual exploitation has been a serious problem throughout history. The Internet exacerbated this problem, making it difficult for law enforcement to investigate. Social media gives abusers ways to connect and find victims, and most technology companies are ignoring the growing problem. The government, law enforcement, and technology companies have worked together to create legislation to combat the issue. While the EARN IT Act does present unique constitutional challenges, it is an effective way to deal with the egregious problem of CSAM and should be passed.

\textsuperscript{202} See \textit{Sitz}, 496 U.S. at 454 (holding that random stops were not constitutional where no empirical evidence suggested such stops would be an effective means of promoting safety and advancing the government’s interest). See also English, \textit{supra} note 82, at 460 (explaining that the state had a significant interest in stopping drunk driving because the practice resulted in thousands of deaths and personal injuries).

\textsuperscript{203} See \textit{Sitz}, 496 U.S. at 454 (noting that because this case does not involve random stops, like in previous unconstitutional situations, and given the use of empirical evidence of the efficacy of the comprehensive stops, the stop is constitutional). See also English, \textit{supra} note 82, at 460 (explaining that there was empirical data to rely on in \textit{Sitz}). “The Court then went on to say that . . . there was empirical data to rely on and an arrest rate of 1.6 percent of all drivers passing through the check point was in fact effective.” \textit{Id.}