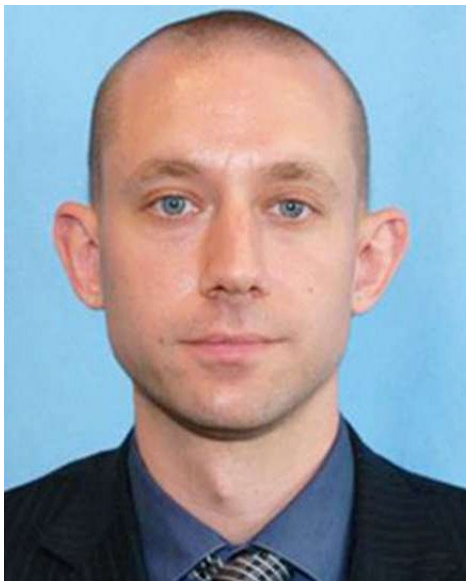
U.S. Department of Justice
Washington D.C.

NATIONAL STRATEGY FOR CHILD EXPLOITATION PREVENTION & INTERDICTION

A Report to Congress - 2023



This report is dedicated to FBI Special Agents Daniel Alfin and Laura Schwartzenberger, two devoted agents who lost their lives while apprehending a perpetrator of violent crimes against children. We will never forget their heroism in defense of children, and we carry on our collective work to prevent these heinous crimes in their honor.

Acknowledgements

This Strategy was made possible due to the unprecedented effort of working groups of subject matter experts that provided their time and insight to the formulation, drafting, and review of 14 core areas relating to child exploitation. The groups produced reports for each area that contain a comprehensive threat assessment and recommendations for action. These reports formed the basis for the following 2023 National Strategy for Child Exploitation Prevention and Interdiction. The Department of Justice wishes to thank all the organizations, agencies, and individuals who made invaluable contributions in the development of this Strategy. Most importantly, we want to thank the survivors and their caretakers who shared their experience and insight with us. We are deeply inspired by your strength.

Cover imagery sourced from freepik.com

Introduction

Preventing and interdicting heinous and destructive acts of child exploitation is extraordinarily difficult work. Child exploitation crimes and the threats facing children have been exploding in scale, complexity, and dangerousness with the rapid expansion of digital technology. While devoted agents, prosecutors, analysts, victim service coordinators, and many other professionals have made significant progress protecting the most vulnerable in our society, there is more work to be done. Combating child exploitation cannot be done by the Department of Justice (the Department) or by the United States government alone. It is an ongoing public health crisis and requires a whole-of-society strategic response. It requires action by Congress, online service providers, non-governmental organizations (NGOs), and foreign partners, and by parents and caregivers as well. In partnership across all levels of government and beyond, the Department will continue its fight to protect children from child exploitation, vindicate the rights of victims, empower survivors, and hold perpetrators accountable.

This National Strategy for Child Exploitation Prevention and Interdiction (National Strategy or Strategy), required by the PROTECT Our Children Act of 2008, builds on prior strategies and reflects the input of survivors and hundreds of subject matter experts from a wide variety of professions. In preparing this strategy, the Department hosted numerous listening sessions comprised of subject matter experts across federal, state, local, and tribal government agencies, law enforcement professionals, academics, and private industry and nonprofit sector professionals, all of whom brought unique backgrounds and perspectives on the dynamics driving child exploitation crimes. Several listening sessions were dedicated to hearing from survivors and caretakers who have been impacted by child exploitation crimes. Those listening sessions, along with countless hours of document formulation, review, and editing among subject matter experts, resulted in the publication of Subject Matter Expert Working Group Reports, each focused on a distinct child exploitation topic:

- Child Sexual Abuse Material
- Child Sex Trafficking in the United States
- Child Exploitation in Special Areas and Populations
- Extraterritorial Child Sexual Abuse
- Livestreaming and Virtual Child Sex Trafficking
- Sextortion, Crowdsourcing, Enticement, and Coercion
- Unique Resource and Enforcement Issues
- Technology
- Offender Psychology
- Partnerships
- Prevention
- Sex Offender Registration Violations
- Survivors, Caretakers, and Access to Survivor Care
- Wellness Challenges for Law Enforcement Personnel

These 14 reports, which are publicly available at https://www.justice.gov/psc/publications-resources, reflect the most pressing dynamics of child exploitation crimes, including the impact

of the global COVID-19 pandemic. Each report contains a detailed threat assessment and recommendations for action. Those reports informed the development of this National Strategy and the strategic solutions contained herein.

The Appendices of the National Strategy fulfill certain statutory reporting requirements and reflect the totality of the federal government's work since 2016, including federal investigations and prosecutions, interagency coordination, grant programs, policy and research initiatives, and other efforts to address the prevention and interdiction of child exploitation offenses. The Appendices also provide details on the Department's legislative proposals and funding for crimes against children.

National Strategy for Child Exploitation Prevention and Interdiction

2023 REPORT TO CONGRESS

We face unprecedented and ever-evolving challenges in the war to protect our children from online sexual exploitation and abuse.[1]

Much has changed since October 2008 when Congress enacted the legislation that requires the National Strategy for Child Exploitation Prevention and Interdiction. PROTECT Our Children Act of 2008, Pub. L. No. 110-401, 122 Stat. 4229 (2008). At the time, Twitter was only two years old, and Facebook only four. The first iPhone was released the year before, with other smartphones coming on the market in the following years. Apple and Google had just launched their app stores, and the Tor Project had just begun developing its browser.[2] Bitcoin would not exist for two more years, and end-to-end encrypted messaging services would not start to emerge for about five years.

Due to these technological advancements, the scale, complexity, and dangerousness of threats facing children today are unprecedented. Simply put, modern technology is the perfect tool for child sex offenders, giving them access to children all over the world and putting them in touch with other child sex offenders with whom to conspire – all while concealing their identities and locations and often, but not always, their activity. The fact is that technology creates two sad realities. On the one hand, law enforcement officers can watch as offenders congregate on the Dark Web, committing child sex offenses in an open and notorious manner with little fear of getting caught. On the other, we are sure in the knowledge that offenders are exploiting children online and in real life -- and are not getting caught because their crimes are shielded by encryption and anonymization. Although we have a qualitative picture of the nature of child sexual exploitation in encrypted and anonymous spaces, and we have evidence suggesting that the threats to children are growing, we have no fulsome quantitative information about its scope and prevalence. What we do not know haunts us.

It is imperative to acknowledge that the benefits of technology that prioritizes encryption, anonymization, co-mingling of adult and child users, and limitless information exchange come with a cost. In the often zero-sum game that shapes the current discussion about technology, efforts to enhance privacy often come with a hidden price: the risk of harm to our children. Children are placed and left in grave danger in these unmonitored, co-mingled, often encrypted, and anonymous spaces. If nothing else, there needs to be more honesty about how society weighs these benefits and costs.

---

[1] The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong? *The New York Times*. Retrieved April 27, 2022, from https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html

[2] The Tor Project is a 501(c)(3) non-profit organization that develops and maintains software for the Tor anonymity network, the most frequently utilized network within the Dark Web.

As one mother of two victims of online child sexual exploitation reported when both her children had to be hospitalized for suicidal thoughts: "Every hope and dream that I worked towards raising my children — completely gone … When you're dealing with that, you're not worried about what somebody got on a college-entrance exam. You just want to make sure they can survive high school, or survive the day."[3] Surveys of survivors conducted by the non-profit organization Thorn and the Canadian Centre for Child Protection (C3P) paint a similar picture of the trauma inflicted on these children.[4]

Over the last few years, we have examined how the threats have evolved through different lenses: child sexual abuse material (CSAM),[5] child sex trafficking in the United States, extraterritorial child sexual exploitation and abuse, technology, offender psychology, victim access to services, prevention, and legal and resource issues, among others. Our assessment does not stand alone. Other similar assessments, including the global threat assessment by WeProtect Global Alliance, have reached similar conclusions.[6] We face a public health crisis on a global scale as the child exploitation threats have grown exponentially in scale, complexity, and dangerousness:

- *Scale*: Today there are more victims and more offenders than ever before, and a seemingly endless stream of CSAM circulating online.

    - Since the enactment of the PROTECT Our Children Act, the number of victims identified in CSAM has risen almost ninefold, from 2,172 victims in March 2009, to over 19,100 as of April 2022.[7] In 2021 alone, due to detailed analysis of newly created CSAM, the National Center for Missing & Exploited Children (NCMEC) alerted law enforcement to over 4,260 potential new victims of CSAM.[8]

    - Steadily increasing each year from FY 2008 to FY 2019, the annual number of defendants federally prosecuted by the Department for producing CSAM nearly tripled. Data from the U.S. Sentencing Commission is even more dramatic,

---

[3] *Child Abusers Run Rampant as Tech Companies Look the Other Way*, Michael H. Keller and Gabriel J.X. Dance, New York Times, November 9, 2019, available at https://www.nytimes.com/interactive/2019/11/09/us/internet-child-sex-abuse.html. *See also* https://www.nytimes.com/2019/11/09/us/online-child-abuse.html.

[4] *See Sextortion: Findings From a Survey of 1,631 Victims,* June 2016, available at https://www.thorn.org/wp-content/uploads/2016/08/Sextortion_Report.pdf; *Survivors' Survey*, 2017, available at https://www.protectchildren.ca/pdfs/C3P_SurvivorsSurveyFullReport2017.pdf.

[5] The term "child pornography" is currently used in federal statutes and is defined as any visual depiction of sexually explicit conduct involving a person less than 18 years old. While this phrase still appears in federal law, "child sexual abuse material" is preferred, as it better reflects the abuse that is depicted in the images and videos and the resulting trauma to the child. In 2016, an international working group, comprising a collection of countries and international organizations working to combat child exploitation, formally recognized "child sexual abuse material" as the preferred term.

[6] *See* Global Threat Assessment 2021, WeProtect Global Alliance, available at https://www.weprotect.org/global-threat-assessment-21/; *see also* Report to Congress, Increasing the Efficacy of Investigations of Online Child Sexual Exploitation, Brian Levine, August 2022, https://nij.ojp.gov/library/publications/fy-2021-report-committees-judiciary-study-investigative-factors-related-online

[7] *See National Strategy for Child Exploitation Prevention and Interdiction*, United States Department of Justice, August 2010, Appendix D, page D-2, available at https://www.justice.gov/psc/docs/natstrategyreport.pdf; https://www.missingkids.org/theissues/csam#bythenumbers.

[8] *See* https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata.

showing a 422% increase in production offenders over the 15 years from FY 2005 (98 defendants) to FY 2019 (512 defendants).[9]

- In 2021, the number of CyberTips concerning child sexual exploitation forwarded to Internet Crimes Against Children (ICAC) Task Forces was over four times higher than the number received in 2016, rising in five years from 83,967 to 371,515. The funding for ICAC Task Forces over that time did not increase at a commensurate pace (increasing only by one-third from $22,000,000 to $29,560,410).

- Relatedly, the Department has also seen increases in the number of victims per offender, who can use technology to ensnare a shocking number of children without ever leaving their home. The approximately one dozen defendants prosecuted through *Operation Subterfuge*, for example, victimized upwards of 1,600 children.[10]

- On the global level, data from NCMEC and C3P reveals a staggering proliferation of CSAM.

    - NCMEC operates the CyberTipline, which receives reports from the public and internet platforms about apparent offenses involving child sexual exploitation. From 2012 to 2021, the volume of CyberTips increased by ***a factor of 70*** (415,650 to 29,309,106). Over those ten years, on three occasions the volume of CyberTips doubled or nearly doubled from one year to the next, and in 2016, the number of CyberTips was four times what it was the prior year.[11]

    - From 2016 to January 5, 2022, C3P sent over 10 million notices to providers alerting them to CSAM found on the providers' platforms. Removal times can sometimes be distressingly sluggish, and most significantly, almost half of the images found are taken down only to be reposted again.[12]

- From 2019-2021, reports of other forms of child sexual exploitation and abuse to the CyberTipline have also increased year over year, in every category.[13]

---

[9] *See Federal Sentencing of Child Pornography: Production Offenses*, United States Sentencing Commission, Oct. 2021, p. 17, available at https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2021/20211013_Production-CP.pdf.

[10] *See* https://www.justice.gov/usao-edva/pr/member-international-child-exploitation-conspiracy-sentenced. The Sentencing Commission report, *supra* at pg. 27, indicates that 40% of defendants sentenced for CSAM production in FY 2019 had more than one victim, with one case involving 440 victims.

[11] *See CyberTipline 2021 Report*, National Center for Missing & Exploited Children, available at https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata.

[12] *See Project Arachnid: Online Availability of Child Sexual Abuse Material*, June 2021, p. 13, Table 6-2 and Table 7-2 available at https://www.protectchildren.ca/pdfs/C3P_ProjectArachnidReport_en.pdf; https://projectarachnid.ca/en/

[13] *See* https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata.

Reporting Category	2019 Reports	2020 Reports	2021 Reports
Extraterritorial Child Sexual Abuse	683	955	1,624
Child Sex Trafficking	11,798	15,879	16,032
Child Sexual Molestation	4,747	11,770	12,458
Online Enticement of Children for Sexual Acts	19,174	37,872	44,155

- *Complexity*: The advent of so many different online platforms with global reach, the proliferation of encryption and anonymizing technology, and the ubiquity and acceptance of the co-mingling of adult and child users, have complicated the identification, interdiction, and investigation of online child sexual exploitation.

    - Smartphones, for example, are fully encrypted devices that fit in a pocket that offenders use to produce, livestream, store remotely, access, send, and receive CSAM, and engage with other offenders or children on any manner of social media and messaging apps.[14]

    - It is becoming increasingly common to encounter offenders like Bud Evers, who possessed over 120 devices with a combined 24 terabytes of storage – an amount of data that would have been unthinkable just a few years ago. Due to the volume of seized evidence, a team of computer forensic experts was required to devise and execute special analytical and forensic protocols to undertake the search.[15]

    - In one case, offenders used over eight different platforms to exploit children, first congregating on Discord, an internet communications service, and then sexually exploiting hundreds of children via web camera or cell phone camera over myriad video-streaming platforms, including Omegle, Skype, live.me, Snapchat, Periscope, musical.ly, YouNow, and others.[16]

    - Offenders easily meet children in online spaces such as Instagram and gaming platforms, and then lure them to messaging apps where the grooming of the child is shielded behind encryption.[17] Once that happens, the investigative trail often goes cold.

    - Investigations and prosecutions of online offenses frequently have a global dimension, as an offender in one country can exploit victims and find like-minded

[14] *See* https://www.justice.gov/usao-mdfl/pr/lakeland-man-sentenced-80-years-prison-producing-and-transporting-child-pornography.
[15] *See* https://www.justice.gov/opa/pr/former-teacher-sentenced-27-years-prison-child-sex-tourism-and-child-pornography-offenses.
[16] *See* https://www.justice.gov/usao-edpa/pr/members-nationwide-child-exploitation-enterprise-sentenced-prison.
[17] *See Video Games and Online Chats Are 'Hunting Grounds' for Sexual Predators*, Nellie Bowles and Michael H. Keller, New York Times, December 7, 2019, available at https://www.nytimes.com/interactive/2019/12/07/us/video-games-child-sex-abuse.html.

offenders in other countries, using platforms that then harbor evidence in yet other countries.

- One British man was convicted of blackmail, voyeurism, making indecent images of children, and encouraging the rape of a child. Although he was convicted of offenses involving approximately 50 children, the investigation suggested that, between 2009 and 2017, he targeted more than 200 victims worldwide, including in the United States. He coerced children to send him photos of themselves engaged in sadistic, masochistic, humiliating, or degrading conduct, which he then would post on "hurtcore" sites on the Dark Web. He was only apprehended after a four-year investigation involving the National Crime Agency and Government Communications Headquarters in the United Kingdom, as well as the U.S. Department of Homeland Security, the Australian Federal Police, Europol, and other law enforcement around the world.[18]

- Similarly, the FBI led *Operation Pacifier,* which targeted a Dark Web-based child exploitation hidden service. The operation resulted in the arrest of 548 foreign individuals and the identification or rescue of 296 children abroad. U.S. law enforcement agencies arrested over 348 individuals based in the United States (including 25 American CSAM producers and 51 American hands-on abusers) and rescued or identified 55 American children.

- A single person can facilitate a massive volume of child exploitation offenses around the world. In the anonymity of the Dark Web, Eric Marques operated a hosting service on Tor that included 200 child exploitation websites that brought together hundreds of thousands of offenders from across the world and housed millions of images of child exploitation material, including images of infants and toddlers involved in bondage, bestiality, and humiliation involving urination, defecation, and vomit. The investigation that led to his arrest involved 70 law enforcement agents from over a dozen countries.[19]

- *Dangerousness*: The Department is encountering younger victims, and more victims who have endured horrific physical violence, than ever before.

[18] *See Matthew Falder: How Global Taskforce Caught Birmingham Paedophile*, Jessica Labhart, BBC News, February 19, 2019, available at https://www.bbc.com/news/uk-england-birmingham-42921977; *see British Paedophile Paul Leighton Jailed for 16 Years*, Kevin Donald, The Guardian, September 4, 2017, available at https://www.theguardian.com/uk-news/2017/sep/04/british-paedophile-paul-leighton-jailed-for-16-years-for-rape

[19] *See* https://www.justice.gov/usao-md/pr/dark-web-child-pornography-facilitator-sentenced-27-years-federal-prison-conspiracy.

- According to data from the U.S. Sentencing Commission, the number of cases involving production of sexually explicit images of an infant or toddler more than quadrupled from 2017 to 2020.[20]

- In 2017, a hidden service on Tor called "Hurtmeh" that was dedicated exclusively to the sadistic and masochistic abuse of children had 800,000 members.

- The Department's cases increasingly involve offenders who threaten victims not only online but also in person. For example, in 2019, four men were sentenced to long prison terms for their involvement running a Tor hidden service called the Giftbox Exchange that included a sub-forum dedicated to the sexual abuse of infants and toddlers. In a separate case, two of those defendants who met through the hidden service were sentenced to life in prison for their rape of a toddler.[21]

The above concerns, and more, led WeProtect Global Alliance to conclude in its 2019 threat assessment that the "scale, severity and complexity of online [child sexual exploitation and abuse] is increasing at a faster pace than those aiming to tackle the activity can respond, with referrals from industry and law enforcement partners reaching record highs. This creates an urgent need for governments, law enforcement organizations, the technology industry and third sector organizations to work together to step up their collective response."[22] Alarmingly, WeProtect reiterated this observation in 2021, writing in stark terms that the "scale of child sexual exploitation and abuse online is increasing. This sustained growth is outstripping our global capacity to respond."[23]

Strategic Response to Date. As demonstrated in the prosecution statistics and case examples provided above, the Department has never waned in its effort to identify, investigate, and prosecute online child sex offenders. As those cases show, we constantly seek to develop cutting-edge investigative techniques to infiltrate and dismantle the online spaces where offenders congregate, normalize one another's sexual interest in children, and promote and facilitate the commission of online child sex offenses. We also must continually adapt as conditions change on the ground, such as with the COVID-19 pandemic.

Beyond investigations and prosecutions, the Department is also tireless in its efforts to provide comprehensive training to ensure there is sufficient investigative and prosecutorial capacity among our federal, state, local, and tribal partners to combat online child sexual exploitation. The flagship of these efforts is the annual National Law Enforcement Training on

---

[20] *Cf. Use of Guidelines and Specific Offense Characteristics*, 2017, p. 44, available at https://www.ussc.gov/sites/default/files/pdf/research-and-publications/federal-sentencing-statistics/guideline-application-frequencies/2017/Use_of_SOC_Guideline_Based.pdf; *Use of Guidelines and Specific Offense* Characteristics, 2020, p. 41, available at https://www.ussc.gov/sites/default/files/pdf/research-and-publications/federal-sentencing-statistics/guideline-application-frequencies/Use_of_SOC_Guideline_Based.pdf

[21] *See* https://www.justice.gov/opa/pr/four-men-sentenced-prison-engaging-child-exploitation-enterprise-tor-network.

[22] *See Global Threat Assessment*, WeProtect Global Alliance, 2019, page 7, available at https://www.weprotect.org/wp-content/uploads/WPGA-Global-Threat-Assessment-2019.pdf. *See also The Annual Report 2020*, Internet Watch Foundation, available at https://annualreport2020.iwf.org.uk/

[23] *See* https://www.weprotect.org/global-threat-assessment-21/#report, page 3.

Child Exploitation, which from 2015-2019 reached a total of almost 7,300 law enforcement personnel, prosecutors, and other professionals working in this field. In 2020 and 2021, the National Training was converted to a virtual format due to the pandemic, and it reached a total of 4,855 personnel. Each year, the agenda is carefully designed to provide instruction on cutting-edge technological and legal issues concerning online child sexual exploitation and abuse.

The Department is also extensively engaged with its international partners to generate a global response to this global crime. This work includes significant support to WeProtect Global Alliance, which seeks to enhance efforts to identify victims, reduce the availability of CSAM online and the re-victimization of children, and increase public awareness of the risks posed by children's activities online. This organization is currently supported by 100 governments, 65 technology companies, 87 civil society organizations, and nine international organizations.

The Department has collaborated extensively with WeProtect Global Alliance on the development of their three signature products: the Global Threat Assessment (referenced above), the Model National Response, and the Global Strategic Response.[24] The Model National Response is designed to enable a country to assess its current response and identify gaps, prioritize national efforts to fill gaps, and enhance international understanding and cooperation. The Global Strategic Response reflects the international nature of the issue and provides objectives and a comprehensive strategy for collaboration, coordination, and shared learning to eliminate online child sexual exploitation and abuse at global and regional levels.

The Department also worked very closely with the Department of Homeland Security and our "Five Country" government counterparts from Australia, Canada, New Zealand, and the United Kingdom to develop and publish in March 2020 the *Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse*.[25] The Voluntary Principles were conceived at the Five Country Ministerial Digital Industry Roundtable on July 30, 2019, in London, where the U.S. Attorney General and the other Five Country Ministers and senior representatives from Facebook, Google, Microsoft, Roblox, Snap, and Twitter agreed that "tackling [the online child sexual abuse] epidemic requires an immediate upscaling of the global response to ensure that all children across the globe are protected…and that there is no safe space online for offenders to operate."

Developed in consultation with several leading technology companies and a broad range of experts from industry, civil society, and academia, the 11 Voluntary Principles outline measures that companies in the technology industry can choose to implement to protect the children who use their platforms from sexual abuse online and to make their platforms more difficult for child sex offenders to exploit. The Voluntary Principles provide a common and consistent framework to guide the digital industry in its efforts to combat the proliferation of online child exploitation.

<u>But more is needed</u>. Despite all of these efforts, our society continues to lose ground in the ability to protect children online. As expressed in both WeProtect Threat Assessments, the growth in online child sexual exploitation is outpacing our capacity to respond. Establishing and

[24] *See* https://www.weprotect.org/frameworks/
[25] *See* https://www.justice.gov/opa/press-release/file/1256061/download

maintaining a work force of specialized law enforcement officers, digital investigative analysts, prosecutors, and victim support personnel are critical, but it always has been and remains a challenge. There are multiple, often-related, aspects of technology that create risk for children and opportunity for offenders, primarily:

- an uneven response to online child safety by the tech sector;
- a CyberTipline system that is overwhelmed;
- anonymization of offenders;
- encryption of data storage and communications;
- online environments where children and adults interact without supervision or controls;
- globalized, often sovereignless, platforms;
- remote, often extraterritorial, storage; and
- a compounding lack of public awareness of these risks.

It is important to understand that these issues are often in tension with one another. Some, such as encryption, anonymization, and sovereignless companies, concern a lack of information because of the all-too-common inability to obtain even basic information to detect or interdict criminal activity or conduct an investigation, despite a lawful warrant or court order. Others, particularly the inconsistent prioritization of child safety, may involve information that is available to platforms but never acted upon or reported to law enforcement. And yet others, especially CyberTips, create an ever-growing volume of information concerning the possession and trading of CSAM far beyond the current ability of law enforcement to address.

We discuss each of these problems in more detail below. But we must emphasize that (1) each must be solved in order to meaningfully address online child sexual exploitation; and (2) none of these problems can be solved *solely* by providing more money or more resources for investigations and prosecutions, nor can they be solved *solely* by the U.S. government. Rather, they require a whole-of-society approach to develop a culture of safety for children online.

Inconsistent Prioritization of Child Safety. While there are many technology companies committed to the protection of children online, data reveals a wildly divergent response by online providers to online child safety. According to NCMEC, in 2019 and 2020, over 1,400 companies were registered to use the CyberTipline. But in 2019, only 148 companies (approximately 10% of registered companies) sent in CyberTips. The results in 2020 are barely any better, with 168 companies sending in CyberTips (approximately 12% of registered companies). Although the number of companies registered to submit reports to the CyberTipline increased in 2021, exceeding 1,800 companies, the response rate remained the same, as only 230 submitted any reports (approximately 12.8% of registered companies).[26]

Looking more closely, the data reveals the massive disparity in the effort by companies across the industry.

[26] https://www.missingkids.org/content/dam/missingkids/pdfs/2019-reports-by-esp.pdf
https://www.missingkids.org/content/dam/missingkids/pdfs/2020-reports-by-esp.pdf
https://www.missingkids.org/content/dam/missingkids/pdfs/2021-reports-by-esp.pdf

- In 2019, 2020, and 2021, a single company—Facebook (now Meta) and its subsidiaries—accounted for approximately 92-95% of all CyberTips sent in by the technology industry (almost 16 million CyberTips in 2019, 20 million in 2020, and almost 27 million in 2021).[27]

- In 2019, 2020, and 2021, just three companies were the source of approximately 98% of all CyberTips (Facebook, Google, and Microsoft in 2019; Facebook, Google, and Snapchat in 2020 and 2021).[28]

- In stark contrast, Apple in 2019, 2020, and 2021 sent in only 205, 265, and 160 CyberTips, respectively. From a shocking mere eight CyberTips in 2019, Amazon's reporting increased in 2020 to 2,235 CyberTips and again in 2021 to 27,204 CyberTips, but it still lags far behind its peers. Setting aside the numbers, discussed in NCMEC's recent 2022 Cybertip Report released in May 2023,[29] there is also a significant difference in the quality of CyberTips. For example, at least 90% of Amazon Photos reports contain no actionable information concerning the user, making the reports almost useless.

- In 2019, 2020, and 2021, the majority of companies (66%, 66%, and 63%, respectively) submitting CyberTips sent in fewer than 100 reports for the year.[30]

This disparity in industry response was part of the motivation behind the development of the Voluntary Principles, discussed above, to urge the technology industry to meaningfully address online child safety. In a statement released on the two-year anniversary of the launch of the Voluntary Principles, the Five Countries emphasized the responsibility the internet industry has to protect children in the online world they have created, and the need for the internet industry to be transparent in how it designs its systems and platforms to promote child safety.[31] On a positive note, there is room for hope. The Tech Coalition, an internet industry led organization, has launched its own "Project Protect" and transparency framework in 2020 and 2021, respectively. Further, recently the Tech Coalition reported that its members have increased their use of filtering systems to detect, remove, and report CSAM.[32]

The CyberTipline System is in Crisis. Although, as explained above, the tech industry as a whole varies wildly with respect to its contributions to the CyberTipline, it is still plainly obvious that the overall rise in the number of CyberTips has been, and continues to be, astronomical. There is little comfort in the fact that the rate of growth has technically slowed in recent years, with increases of roughly 28% from 2019 to 2020, and 35% from 2020 to 2021 (as

[27] *Id*. The 2019 and 2020 data for Facebook includes all subsidiaries combined. In 2021, the data is divided into the parent company and its subsidiaries: Facebook, Instagram, Novi, and WhatsApp.
[28] *Id*.
[29] *See* https://www.missingkids.org/cybertiplinedata
[30] *Id*.
[31] *See* https://www.justice.gov/criminal-ceos/file/1490676/download
[32] *See* https://www.technologycoalition.org/newsroom/the-tech-coalition-announces-project-protect; https://www.technologycoalition.org/newsroom/tech-coalition-launches-trust-voluntary-framework-for-industry-transparency; https://www.technologycoalition.org/annual-report.

compared to the period from 2013 to 2018 where the numbers repeatedly doubled, or more, from year to year). But when the baseline is tens of millions of CyberTips, even a modest percentage increase from one year to the next translates to millions more leads every year.

In addition to the ever-rising volume, the CyberTipline also has a qualitative problem. From one tip to the next, the content of the information varies wildly, with some tips containing so little that it requires additional investigative effort just to determine where the tip should be sent or whether the tip is viable at all because it lacks any user attribute information. Images virally distributed can swamp the system. Multiple leads involving a single offender may lead to duplication of efforts.

This is resulting in a crisis. In the United States, the number of CyberTips referred to the ICAC Task Forces has more than quadrupled in six years. At the same time, their resources have only increased a modest 34%. This mismatch between crime reports and law enforcement resources puts ICAC Task Forces in an untenable position. They feel an obligation to investigate every CyberTip they receive without regard to its quality. *See* 34 U.S.C. § 21114(8). But they are not given the resources to keep up with the growth of CyberTips. At the same time, they must make triaging decisions based on woefully inadequate information. Compounding these challenges are developments in the law that often require additional investigative steps and legal process. Furthermore, unlike the tech industry and NCMEC, ICAC Task Forces operate without civil immunity to protect them in the event of a good-faith error. *Cf.* 18 U.S.C. §§ 2258B and 2258D.

Work is being done to try to address this issue. In the last two years, for example, NCMEC has instituted measures within the CyberTipline system to assist with deconfliction, deduplication, triaging, and automation, all of which seek to improve the efficiency of the law enforcement response. Yet even with these improvements, ICAC Task Forces, as our first responders to CyberTips, continue to lack adequate tools and resources to properly respond.

Anonymization. Few can debate the clear and grave threat to children posed by the Dark Web, as vividly illustrated in the examples provided above. Protected from identification and geolocation, offenders can congregate on the Dark Web and engage in child sexual exploitation for years in an open and notorious manner with little to no fear of getting caught. Despite these obvious harms, one such Dark Web platform, the Tor Project, continues to be supported by taxpayer dollars.[33] As proud as we are of our Dark Web prosecutions, they do not offer a systemic solution to the near perfect utility of the Dark Web for child sex offenders.

Encryption. Similarly, certain implementations of encryption are unintentionally benefitting child sex offenders by shielding their crimes from detection and preventing fulsome investigation by preventing law enforcement from accessing evidence, even pursuant to valid court orders or warrants. For example, the reason Facebook generates so many CyberTips a year is because they voluntarily scan their platforms to find and remove files that match known CSAM. In 2019, Facebook announced its intent to adopt end-to-end encryption on its messenger platform. At the time of that announcement, NCMEC estimated that if Facebook made that

[33] *See* https://support.torproject.org/misc/misc-3/

change, 12 million CyberTips would disappear. The crimes would not stop, but Facebook's ability to detect them would.

As another example, consider ProtonMail. According to ProtonMail's website, it is the world's largest encrypted email provider, which stores all of its data in Switzerland, and it has engineered its service in such a way that it cannot scan the content of users' messages. As a result, images of child exploitation, and messages concerning grooming of children for sexual purposes or sextortion cannot be detected. At one time, ProtonMail advertised its services as being difficult for even law enforcement agencies to investigate any crimes that may be committed using the service by placing what limited data it does store beyond the reach of most countries' laws. As previously advertised on its website:

> All user data is protected by the Swiss Federal Data Protection Act (DPA) and the Swiss Federal Data Protection Ordinance (DPO) which offers some of the strongest privacy protection in the world for both individuals and corporations. As ProtonMail is outside of US and EU jurisdiction, only a court order from the Cantonal Court of Geneva or the Swiss Federal Supreme Court can compel us to release the extremely limited user information we have.

Through their apparent total pursuit of their users' privacy, companies such as ProtonMail inevitably create online services that allow child exploitation offenders to hide, and therefore undermine law enforcement and public safety efforts to protect children. In fact, ProtonMail was used by Alexander Nathan Barter when he planned his travel to rape, kill, and eat a 13-year-old child.[34] Barter was only apprehended because he conversed with an undercover law enforcement officer.[35]

Co-mingled Online Environments where Children and Adults Interact as Peers. In real life, parents would never take children, especially children under the age of 12, to a mall or park and leave them there unsupervised with adult strangers. Yet the virtual equivalent happens online every day. Particularly on gaming and livestreaming platforms, children and adults can interact as a matter of course, sometimes knowingly (where the adult presents himself as an adult) and sometimes unknowingly (when the adult lies about his or her age and poses as a child). Some platforms that are specifically designed for children deploy significant guard rails to keep children safe. But this can create a false sense of security, as platforms can do little to prevent offenders from luring children to different online spaces where no such safety mechanisms are in place. We cannot overstate the danger that this creates, particularly as children use more and more online platforms at younger and younger ages, especially following the COVID-19 era. Parents may not know the extent of their responsibility to be vigilant about their children's online interactions, particularly when app stores advertise common platforms that bear misleading age ratings like 12+ or teen (ostensibly signaling appropriateness for that age but actually meaning something different).[36]

---

[34] *See* https://www.justice.gov/usao-edtx/pr/dark-web-cannibal-sentenced-40-years-followed-lifetime-supervised-release

[35] More information about the Department's work concerning lawful access is available at https://www.justice.gov/olp/lawful-access

[36] *See* https://protectchildren.ca/en/resources-research/app-age-ratings-report/

Global, Sovereignless Platforms. Some technology providers frustrate government's lawful access to information by designing operations to be essentially sovereignless, meaning they are beyond the reach of legal requests for information from any country. For example, Telegram is a Dubai-based encrypted cloud-based mobile and desktop messaging app that purposefully stores data in multiple jurisdictions around the globe, specifically so that law enforcement must obtain several court orders from different jurisdictions in order to obtain any useable information. As Telegram explains on its website, since its launch in 2013, it has provided zero bytes of data in response to any lawful government request, in part because "Telegram uses a distributed infrastructure. Cloud chat data is stored in multiple data centers around the globe that are controlled by different legal entities spread across different jurisdictions. The relevant decryption keys are split into parts and are never kept in the same place as the data they protect. As a result, several court orders from different jurisdictions are required to force us to give up any data."[37]

By protecting privacy at all costs, companies such as Telegram unavoidably facilitate criminal activity and undermine law enforcement and public safety efforts. Titus Miller, for example, used Telegram to exchange CSAM with other like-minded offenders.[38] Investigators later discovered that he had also repeatedly filmed himself raping children aged 4-6 who were in his care through his employment at a child day care center. Ultimately, Miller was sentenced to 100 years in prison. Miller's crimes were uncovered because an offender caught in a separate investigation told law enforcement he was corresponding with Miller on Telegram and allowed law enforcement to use his Telegram account in an undercover capacity to further the investigation of Miller. As with Barter, Miller's crimes were only detected through chance.

In addition, a single foreign provider can facilitate a massive amount of child sexual exploitation. As noted above, the C3P operates *Project Arachnid*, a web crawler that searches for known CSAM. When such material is detected, C3P sends a notice to the provider asking that the material be removed. In its comprehensive report on the first few years of Project Arachnid, C3P indicated that it sent notices about CSAM to over 760 electronic service providers worldwide. However, close to half of all CSAM detections (48%) were linked to a single file-hosting service operated by one French telecommunications company—Free.fr.[39]

The simple fact is that these foreign companies create products that are being used to endanger and harm American children. And as foreign companies, they are beyond any "whole-of-government" approach focused solely within the United States.

Insufficient Forensic Capacity. One of the most critical gaps in the technology arena continues to be the lack of sufficient computer forensic resources. The volume of computer data has increased exponentially with gigabytes of stored data becoming terabytes. In addition, the volume of devices located during searches has significantly increased. It is now routine for homes to contain over a dozen desktops, laptops, tablets, smart phones, and/or external storage devices. Each device requires some analysis, even if just to eliminate it as potential evidence,

[37] *See* https://telegram.org/faq#q-do-you-process-data-requests
[38] *See* https://www.justice.gov/usao-ne/pr/lincoln-man-receives-100-year-sentence-producing-child-pornography
[39] *See* https://www.protectchildren.ca/en/resources-research/project-arachnid-csam-online-availability/.

which adds to the time spent on each case. Another difficulty is the reality that nearly all types of criminal cases now require some computer forensic analysis, greatly straining agency resources that might otherwise be available for child exploitation cases, while the number of child exploitation cases requiring computer forensic analysis also continues to grow. For example, over the six-year period of FY2016 – FY2021, the number of Child Exploitation Cases received by the FBI's Regional Computer Forensics Laboratories (RCFLs) has *nearly doubled* from more than 5,000 to more than 10,000,[40] and the number of computer forensic examinations conducted by the ICAC Task forces *increased by 17%* from more than 77,000 to more than 90,000.[41] In far too many instances the result is a significant – up to years long – delay between when devices and data are seized by law enforcement and criminal charges are able to be brought against a perpetrator.[42]

Remote Storage. The advent of online storage options also undermines child safety in two ways. First, as Free.fr demonstrates, one company, anywhere in the world, can effectively set the standard, or the absence of any standards at all, with respect to online child safety. There is little that law enforcement in the United States can do to change how a foreign company operates. Instead, as offenders increasingly flock to a preferred platform to commit their crimes, law enforcement is left trying to keep pace. To provide a sense of scale, over one million depictions of child sexual abuse and harmful content were hosted on Free.fr, and nearly three million such images and videos were traced to that site, according to C3P.[43]

Second, the existence of a stable, enduring online repository of CSAM allows offenders to easily commit their crimes, form a community, bond with one another, and validate and normalize their abhorrent sexual interest in children. As explained in the 2021 WeProtect Global Alliance Threat Assessment:

> Offender populations have come to rely on the ease of use, security and privacy of cloud file sharing apps to store and distribute illegal images and videos. Cloud storage makes it possible to share child sexual abuse material by simply posting a link in a forum, on a platform or through direct messaging, to thereby reach more offenders, more quickly… Perpetrators typically use cloud file sharing to efficiently exchange images and videos with both known and new offender contacts. To ensure that content remains accessible for as long as possible, determined offenders use multiple cloud platforms simultaneously. The true nature of harmful links is hidden behind a smoke screen of

---

[40] *See* RCFL Child Exploitation Cases by year table in Appendix C.

[41] There were 77,201 total ICAC computer forensic examinations in FY2016 and 90,318 in FY2021. *See, generally,* ICAC Task Force Forensic Examinations Performed for FY2017-2021 in Appendix F.

[42] Computer forensics and digital investigation is a step-by-step process that is often also iterative in nature. *See* generally, Carroll, O., Brannon, S., & Song, T. "Computer Forensics: Digital Forensic Analysis Methodology." United States Attorney's Bulletin 56, no. 1 (January 2008): pp. 1-8 available at: https://www.justice.gov/sites/default/files/usao/legacy/2008/02/04/usab5601.pdf There are many points at which progress in completing or beginning a step may be delayed and many reasons for delay, including a lack of availability of necessary personnel and the lack of availability or access to necessary tools and equipment. Any delay at any point in the process that is occasioned by such a lack could rightly be characterized as a "backlog" and is something that is difficult, if not impossible, to meaningfully measure.

[43] *Id.*

references to other (lesser) illegal activity or legitimate file-sharing uses to evade detection.[44]

The Department's own cases corroborate this pattern, such as the prosecution of Bryan Thompson, who (in addition to recording his sexual abuse of children and possessing CSAM on several different digital devices) distributed nearly 1,000 images of children engaged in bestiality and sadistic and masochistic conduct by sharing links to his Mega account (a web-based platform offering encrypted data storage).[45] Thompson was only discovered because he communicated with an FBI online undercover employee on a different platform.

While offenders continue to use online spaces insulated from the reach of legal process, or new technologies specifically designed to hide their activities, the online threat to children will continue to grow exponentially if law enforcement is only able to infiltrate a fraction of abuses.

Public Awareness and Market Demand. Compounding all of these challenges is the lack of public awareness of the risks to children. There is a need to educate parents, other caregivers, and children about how to keep children safe online and to provide them with better information to accurately assess dangers. Such awareness-raising is a key component of the Department's Project Safe Childhood.[46] Increased user awareness of actual risks could drive market demand for safer products. However, in many instances, parents and children have very little information about online safety. For example, Apple distributes the ProtonMail app through its store. Although ProtonMail can be used by criminals like Alexander Nathan Barter, discussed above, Apple rates this app as "4+" meaning "apps in this category have no objectionable content." Since ProtonMail is fully encrypted, neither ProtonMail nor Apple has any reliable means to assess the content on that platform. Yet parents see the "4+" rating and may naturally assume that this app is perfectly safe for even the youngest children. This false sense of security, and the promotion of the benefits of privacy without mentioning its costs, stymies the power of the market to demand better.

***

As detailed above, advances in technology have fueled child sexual exploitation, particularly to the extent that technology drives the development of wholly new forms of offenses in which children are preyed upon virtually by offenders who may be thousands of miles away or in different countries. However, we cannot lose sight of the fact that online child sexual exploitation is intertwined with corresponding exploitation and abuse in the physical world. In order to comprehensively respond to the threats of child exploitation, we must address the following trends in both technology-facilitated and in-person child sexual abuse and exploitation.

---

[44] *See* https://www.weprotect.org/global-threat-assessment-21/.
[45] *See* https://www.justice.gov/usao-sdal/pr/grand-bay-man-sentenced-thirty-five-years-prison-child-pornography-case. *See also* https://www.justice.gov/usao-sdny/pr/us-attorney-announces-charges-against-west-point-staff-sergeant-distributing-child
[46] *See* https://www.justice.gov/psc

Child Sex Trafficking in the United States

Child sex trafficking is defined under federal law as the recruiting, enticing, harboring, transporting, providing, obtaining, advertising, maintaining, patronizing, or soliciting of a person under 18 years of age, knowing or recklessly disregarding that the minor will be caused to engage in a commercial sex act or benefitting, financially or by receiving anything of value, from participation in a venture engaged in any of these acts. 18 U.S.C. § 1591(a).

- Federal prosecutions of child-only sex trafficking cases increased 17% from 2019 to 2020, and children made up 69% of victims in all new sex trafficking cases in 2020.[47]
- Looking specifically at federal sex trafficking cases prosecuted in 2020, just over half of the victims were children,[48] with victim ages ranging from 4 to 17 years old when they were exploited, with an average age of 15 years old.[49] 89% of child victims in active sex trafficking cases were between 14 and 17 years old.[50]
- In 2020, 89% of all sex trafficking prosecutions against buyers involved actual or purported child victims.[51]
- The majority (83%) of 2020 active sex trafficking cases involved the internet as the primary method of solicitation, continuing a longstanding trend. Although online solicitation of buyers has been a constant for many years, the websites and apps traffickers use change considerably year over year.[52]
- Only 5% (28) of active sex trafficking cases in 2020 involved exploitation directed by gangs or more formal organized crime groups. Instead, most cases involved individual traffickers exploiting victims without direction from or connection to a larger criminal network. Approximately 43% of victims knew their trafficker prior to becoming a victim.[53]

Extraterritorial Child Sexual Exploitation

Extraterritorial child sexual exploitation and abuse occurs when perpetrators engage in sex acts with children, or produce CSAM, outside the United States.

- Since 2007, U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) has been conducting Operation Angel Watch, which notifies foreign countries regarding the anticipated travel of registered child sex offenders. Even during a period of declining international travel due to the COVID-19 pandemic, the number of leads and notifications processed by the Angel Watch

[47] Kyleigh Feehs & Alyssa Currier Wheeler, 2020 Federal Human Trafficking Report, Human Trafficking Institute (2021), available at https://traffickinginstitute.org/wp-content/uploads/2022/09/2021-Federal-Human-Trafficking-Report-WEB-1.pdf
[48] *Id.* at p. 5
[49] *Id.*
[50] *Id.* at p. 33
[51] *Id*.
[52] *Id*. at pp. 48, 50, 51.
[53] *Id.* at pp. 5, 43.

Center (AWC) remained relatively stable. In 2021, AWC submitted over 2,000 notifications.

- Offenders often gain access to children by working in positions of trust, such as missionaries, religious leaders, leaders or founders of orphanages, or foreign aid providers. Humanitarian workers are often given unsupervised access to children, who are desperate for food, shelter, and attention. The children under their care are often placed in an impossible predicament – endure abuse or risk losing their care.

Abuse on Federal Lands and in Federal Facilities

Child sexual assault occurs on federal lands and in federal facilities, including in Indian country, on military installations, in federal facilities housing unaccompanied noncitizen children, and on commercial flights and cruise ships.

- According to the most recent 2019 National Child Abuse and Neglect Data System (NCANDS), American Indian and Alaska Native (AI/AN) children are 50% more likely to be victims of sexual abuse than Caucasian children. In addition, AI/AN youth are four times more likely to experience multiple victimizations.[54] The long-term impacts of this abuse are profound. Adverse childhood experiences (ACEs) like child sexual abuse are linked to chronic health problems, mental illness, and substance abuse problems in adulthood and can negatively impact education, job opportunities, and earning potential. For many reasons, adequate resources and safe spaces for child victims of sexual abuse to disclose and report may not be readily available in Indian country. The investigation and prosecution of child exploitation crimes in Indian country are complex and require a multi-jurisdictional and multidisciplinary approach.

- There are challenges in responding to incidents of problematic sexual behavior in children and youth, including juvenile-on-juvenile sexual abuse, occurring on military installations and overseas. Federal law and policy is that juvenile matters should be handled by state authorities whenever possible because the States are in the best position to do so. Yet, military children are often deprived of access to the state's juvenile justice system and rehabilitative programs because the incident occurred in an area of military installation where there is "exclusive federal jurisdiction."

- When unaccompanied noncitizen children arrive at the United States' international borders, they are generally transferred into the custody of the U.S. Department of Health and Human Services' Office of Refugee Resettlement (HHS/ORR). ORR facilitates the minor's placement with a vetted sponsor while they await their immigration proceedings. However, such placement can sometimes take time, so

[54] Multiple victimized youth were those who endured multiple discrete episodes of sexual or physical assault and both sexual and physical assault. Tomika N. Stevens et al., Variables Differentiating Singly and Multiply Victimized Youth: Results From the National Survey of Adolescents and Implications for Secondary Prevention, 10(3) Child Maltreatment 211, 219.

ORR funds a network of facilities to care for unaccompanied minors until they are released to a vetted sponsor, or otherwise leave ORR custody. ORR requires all care provider facilities to report significant incidents affecting a minor's health, well-being, or safety within 24 hours, to include possible sexual abuse or human trafficking. [55] In June 2020, HHS's Office of the Inspector General (OIG) published a report titled, *The Office of Refugee Resettlement's Incident Reporting System Is Not Effectively Capturing Data To Assist Its Efforts To Ensure the Safety of Minors in HHS Custody*.[56] HHS has been working to implement the recommendations set forth by OIG to systematically identify and report significant incidents to safeguard children.

Livestreaming Child Sexual Exploitation (LCSE)

Livestreaming child sexual exploitation (LCSE) occurs when an offender compels a child victim to engage in sexually explicit conduct during a broadcast, in real time, to one or more viewers. There are generally three types of LCSE: child "self-generated," offender-streaming, and virtual child sex trafficking.

- **Child "Self-Generated":** This type of LCSE occurs when an offender coerces, tricks, or otherwise compels children to engage in sexually explicit conduct on a livestream, typically from the child's bedroom or a bathroom. In some cases, this activity occurs under the pretext of the offender and victim being in a romantic relationship.

- **Offender-streaming:** Offender-streaming LCSE occurs when an offender sexually abuses a child in person while livestreaming the abuse to viewers. The offender is usually someone who knows, and has easy access to, the victim, such as a family member or a family friend. The viewers may not know each other in real life. They often participate in the activity by requesting that specific sex acts be committed.

- **Virtual Child Sex Trafficking:** In this form of LCSE, offenders pay to watch while another offender sexually abuses a child in person or offenders pay a victim directly to create "self-generated" CSAM. Because of the interactive nature of livestreaming platforms, offenders can request specific sexual abuse acts for an additional cost. Payment is usually made digitally. This offense often involves offenders in the United States and facilitators and children in foreign countries. Children may be transported from rural areas of that foreign country to urban settings in furtherance of this crime.

[55] Standards to Prevent, Detect, and Respond to Sexual Abuse and Sexual Harassment Involving Unaccompanied Children, Office of Refugee Resettlement, Department of Health and Human Services https://www.acf.hhs.gov/orr/standards-prevent-uac-sexual-abuse

[56] OIG Final Report: *The Office of Refugee Resettlement's Incident Reporting System Is Not Effectively Capturing Data to Assist Its Efforts To Ensure the Safety of Minors in HHS Custody*, OEI-909-18-00430, June 2020 (https://oig.hhs.gov/oei/reports/oei-09-18-00430.asp).

Sextortion, Crowdsourcing, and Online Enticement and Coercion

Offenders use a variety of techniques to induce or compel children to record, photograph, or livestream themselves engaging in sexual activity, including deception, threats, or other forms of coercion, sometimes working with other offenders.

- **Sextortion** occurs when offenders use threats or coercive tactics to cause victims to produce and send sexually explicit imagery of themselves. Offenders may use grooming techniques, or basic trickery, to manipulate victims into providing nude or partially nude images or videos of themselves, which they then use to coerce victims into sending more graphic images and videos or pay a ransom. Or they may use other techniques to obtain access to other private and sensitive information, such as using social engineering to compromise social media accounts, school information, friend lists, and other personal information. The perpetrators often threaten to post the images or sensitive information publicly, or send them to the victim's friends and family if the child does not comply with their demands to send more sexually explicit images or videos, or pay a ransom to avoid having the images distributed. From May 2022 to October 2022, U.S. law enforcement and NCMEC witnessed an alarming increase in CyberTips and reports where minor boys have been sextorted for money. Tragically, over a dozen of these boys committed suicide because of the desperation they felt from the threats of sexually explicit images sent to friends and family.[57]

- **Crowdsourcing** in the child sexual exploitation context refers to offenders working together to identify social media profiles of minor victims and strategizing how to convince minors to engage in sexually explicit activity. Often, at least one offender poses as a minor, so the victims believe they are trading sexually explicit content with a same-age peer. This can occur over any social media application and involve traditional images and videos, but livestreaming applications tend to be the preferred platform among crowdsourcing offenders. Crowdsourced child sexual exploitation allows offenders to collaborate with other perpetrators to sexually exploit thousands of minors in short periods of time.
- **Online Enticement and Coercion** may begin with offenders grooming their victims. The sexual grooming process includes identifying a minor, establishing a connection by offering support and attention to the minor, befriending them, gaining their trust, gathering personal information about them, exploiting any emotional vulnerabilities they may have, and lowering their inhibitions by talking, joking, and teaching a minor about sex. In the online context, the sexual grooming period can be very short. Some minors report chatting with offenders for less than an hour before being asked to send sexually explicit images and videos of themselves. Because minors today may feel more comfortable chatting and sending images and videos

[57] *See, e.g.,* An Instagram Sextortionist Tricked 30 Boys into Sharing Intimate Photos. One Took His Own Life, Thomas Brewster, Forbes, August 25, 2022, available at https://www.forbes.com/sites/thomasbrewster/2022/08/25/instagram-sextortionist-fbi-investigation/?sh=cfd09e96fc32; https://www.fbi.gov/news/press-releases/fbi-and-partners-issue-national-public-safety-alert-on-financial-sextortion-schemes

over the internet, long-term sexual grooming is often unnecessary.

- Offenders often groom their victims by posing as a peer. Pretending to be minor boys and girls, offenders will stream pre-recorded videos (often referred to as loops) of other minors engaged in sexual acts to the targeted victim to trick the minor into believing they are watching a live video of someone their own age. This normalizes the sexual behavior and makes children feel more comfortable exposing themselves over a broadcast. Using peer pressure, an offender convinces the minor to engage in sexual acts like those shown to them on the pre-recorded videos. The minor victim may be unaware he or she is communicating with an adult and that the adult is recording the minor's sexually explicit activity.

***

Strategic Solutions

The alarming state of the threat against children demands comprehensive, serious action. We are suffering a public health crisis on a global scale. Political leaders, technology companies, governmental agencies, and society must get serious about the safety risks that modern technology poses to children. Until that happens, we will continue to lose ground, to the detriment of children. Above all, there needs to be a meaningful reckoning with the way offenders can use technology to harm children, and an honest conversation about how to mitigate that harm in a way that preserves technology's benefits. Specifically, we need to engage in a thoughtful conversation about how to protect both privacy and children, the relative risks of all possible solutions, and what is actually gained or lost when child safety features are designed and added. In short, online child safety must be made a co-equal of privacy, and all parties must foster an honest commitment to develop policy and technological solutions that honor both principles. The Department welcomes the opportunity to have that conversation.

Aside from that general mandate, there are 10 major categories of goals common to addressing each child exploitation topic:

- Legislation
- Funding
- Enforcement
- Training
- Technology
- Collaboration
- Research
- Prevention
- Reporting
- Victim Services

Although this document is entitled a National Strategy, it also constitutes a call to action. The solutions to address child exploitation require action not just from the Department of Justice

and law enforcement partners, but also from Congress, the technology industry, our NGO and interagency partners, and others. The Department is poised to coordinate and assist with this work, but cannot compel it. For that reason, the National Strategy does not detail specific steps that may be needed to achieve each solution or set artificial timelines to take those steps. While action is urgently needed, we do not wish to incentivize completion of quick tasks at the expense of the harder work that may yield the most meaningful long-term gains.

Legislation: There is much that Congress can do to better protect children online, including the proposed legislative reforms detailed in Appendix I. Such measures include:

- permit victims of CSAM to pursue civil remedies against online providers;
- better account for the severity of child sexual abuse offenses by updating the U.S. Sentencing Guidelines applicable to such offenses;
- require certain child-serving organizations to report apparent instances of child abuse;
- provide a long-overdue update to the terminology used to describe these offenses by eliminating the phrase "child pornography" from federal law;
- ensure military children are no longer deprived of access to a state's juvenile justice system when an incident occurs in exclusive federal jurisdiction, on any military installation, or overseas;
- close gaps in, and correct adverse judicial decisions concerning federal criminal provisions; and
- enact provisions designed to afford child victims better protections in the federal criminal justice system.

Funding: There is a need for funding with respect to every aspect of the Department's efforts to address child sexual exploitation, from prevention to interdiction to investigation to victim recovery. Historic funding levels are reflected in Appendix K and highlight the generally stagnant or minimal increases in funding since 2016 despite the notable changes in how online child exploitation is harming children. Priorities include:

- ensuring the funding for ICAC task forces is commensurate to the increase in the scale of domestic child sexual exploitation online and CyberTip response system;
- improving technology, including forensic analytical capacity, that helps law enforcement identify and investigate offenders;
- expanding victim services programs;
- enhancing state, local, and tribal partnership and training programs; and
- building a national prevention campaign, with coordinated outreach among stakeholders, that highlights the desperate need for online child safety.

Enforcement: Enforcement-related measures are needed to deepen the capabilities of federal, state, local, tribal, and foreign law enforcement, prosecutors, and victim-witness personnel. This can be achieved through measures that include:

- developing technical tools for law enforcement to conduct investigations more efficiently;

- building capacity among all relevant personnel to investigate and prosecute child abuse in Indian country;
- improving coordination, including through rapid, technology-facilitated mechanisms, among state, federal, and international law enforcement; and
- ensuring sustainability for state-led human trafficking task forces

Training: There is constant turnover among professionals in this field, particularly due to the emotionally draining nature of the work. In addition, technology is constantly evolving and presenting new ways to commit or hide offenses. The combined effect of these factors creates a constant need to build capacity, both domestically and internationally. Accordingly, a fulsome training agenda is needed aimed at a wide variety of professionals, including:

- enhanced coordination and dedicated funding for the Department-sponsored National Law Enforcement Training on Child Exploitation;
- training improvements for federal, military, state, local, tribal, and foreign law enforcement and prosecutors;
- mapping training efforts to improve efficiency and reduce redundancy;
- training the judiciary on the full range of child sexual exploitation crimes, victim impact, and online technologies; and
- training on child exploitation for all staff caring for unaccompanied minors, personnel responsible for supervising convicted sex offenders, and individuals in licensed professions who may encounter exploited children.

Technology: Even as technology may exacerbate online child sexual exploitation, so too may it be used to combat these crimes. Technological solutions can improve our response, including:

- developing tools to detect new CSAM or livestreaming offenses;
- developing tools to facilitate more efficient law enforcement investigations including the use of hash-based technologies for image and video analysis;
- modernizing case management systems;
- expanding forensic capacity to obtain and analyze evidence on digital devices and in the cloud, including in encrypted environments; and
- providing more robust online safety measures focused on prevention and interdiction.

Collaboration: Government cannot stop online child sexual exploitation on its own. A whole-of-society approach is essential to any effective solution, including:

- fostering greater collaboration and engagement with the technology industry, whether to improve reporting to the CyberTipline or to detect and interdict livestreamed child exploitation;
- improving standards and transparency of internet platforms for detection and reporting of child sexual exploitation, and maintaining engagement with the tech industry on the Voluntary Principles;

- expanding the use of collaborative task force models in Indian country investigations, and increasing the number of Special Assistant U.S. Attorneys prosecuting child exploitation crimes in Indian country;
- developing an interagency working group to address wellness for professionals handling child exploitation matters;
- improving international cooperation and capacity for investigations of child exploitation outside the United States;
- engaging with partners, including NGOs, to support a trauma- and survivor-informed response to delivering victim services;
- collaborating with the tourism industry and foreign NGOs to prevent and address child exploitation and abuse committed by Americans abroad;
- coordinating with the mental health community to establish a standardized credentialing program for sex offender treatment providers that would apply across jurisdictions; and
- implementing child safety standards and audits for youth-serving institutions and organizations that receive federal funds or seek not-for-profit tax exemption.

Research: Research plays a critical role both with respect to developing a more fulsome understanding of a range of topics, including the needs of victims, the dynamics of offenses, and the psychology of offenders (particularly with respect to developing new tools and standards). Research needs include:

- prevalence studies regarding online platforms where children experience exploitation and the nature of those harms;
- feasibility studies concerning online safety by design;
- development of trauma-responsive standards of care for child exploitation survivors;
- identification of best practices for youth protection within youth-serving institutions and organizations;
- establishment of appropriate, empirically-based standards for the clinical assessment and treatment of sex offenders; and
- assessment of the impact of race, poverty, sex, and sexual orientation and gender identity on the identification of, and response to, child exploitation victims and provision of services.

Prevention: For all of society to do its part to address child sexual exploitation and protect its victims, society must be educated about the crimes. Therefore, a key element to addressing child exploitation is prevention, with measures such as:

- building a national prevention campaign, with coordinated outreach among stakeholders, that highlights the desperate need for online child safety;
- mapping prevention efforts required or provided by states, federal agencies, and NGOs;

- designing and implementing updated educational resources for community members, including parents and guardians, teachers, day-care workers, and health professionals;
- educating teens and parents about detecting and disengaging from online grooming; and
- educating legislators and the judiciary about child sex offenders and child sexual exploitation crimes.

Reporting: If people or entities that possess information that a child is at risk do nothing, then that child cannot be rescued from an exploitive or abusive situation. Improvements to increase reporting of child sexual exploitation and abuse are needed, key among them:

- measures that improve the CyberTipline system and support sharing of information among NCMEC and members of the tech sector interested in detecting CSAM on their systems;
- increased reporting of missing and at-risk children (including providing needed resources to do so);
- updated reporting guidance on unaccompanied minors;
- increased reporting of sexual assaults on cruise ships and commercial flights;
- establishment that all child-focused entities receiving 501(c)(3) tax exempt status are mandatory reporters;
- development of reporting standards as part of the licensing process for relevant industries; and
- improved victim identification with screening across health, social services, and juvenile justice systems.

Victim Services: If the highest aspiration is to prevent child exploitation in the first place, the second highest is to provide victims the support they need to heal and thrive. To that end, it is necessary to:

- encourage the adoption of a whole-of-family approach to service delivery;
- bolster community-based support;
- improve victim identification;
- ensure child victim rights, particularly the right to privacy and safety, during the investigation and prosecution of cases;
- expand and enhance child advocacy centers for child victims and their families nationwide (including on military bases and in other federal jurisdictions) so that every child victim has access to high-quality care;
- enhance approaches to survivor health and well-being;
- identify and utilize funding sources to support the development and operation of housing for minors who have experienced or are at risk of child sexual exploitation, including child sex trafficking; and
- develop best practices on how to incorporate survivors into organizations and partnerships.

***

As explained above, the goals and solutions set forth in this National Strategy are not just for the government, and instead constitute a call to action requiring measures by Congress, the technology industry, our NGO and industry partners, as well as others to address these threats effectively and collaboratively. Many of these goals do not lend themselves to specific timelines or measurable objectives and cannot be accomplished by the Department alone. Swift and efficient action is needed by all relevant stakeholders with the power to act in order to meaningfully thwart the threats to our children and protect them on and offline. While the situation is dire, with the assessments provided by this National Strategy as a guide, the Department is prepared to do its part to prevent and stop child sexual exploitation, hold offenders accountable, and protect victims.