Technology

One of the most persistent, evolving threats to children online is the very technology that enables the digital world to thrive. While technology has many benefits, it also has made it dramatically easier for offenders to harm kids and connect with one another. Those who seek to exploit children can connect on internet networks and forums to produce, sell, share, and trade child sexual abuse materials (CSAM), and to find and groom children for sexual abuse. These interactions are facilitated through numerous forms of internet technology, including websites, email, peer-to-peer networks, internet gaming sites, social networking sites, messaging apps, anonymized networks, instant messaging, Internet Relay Chat (IRC), newsgroups, and bulletin boards. The emergence of these online communities has promoted communication between offenders in ways previously inconceivable in real life. The communities normalize and radicalize an offender's sexual interest in children, facilitate sharing knowledge and best practices among offenders on how to avoid detection or sexually abuse children, and desensitize them to the physical and psychological damages inflicted on the children being exploited.

> *We already know that social media is used to groom, lure, abuse and exploit children. Implementing available technology that would allow industry to continue to work side by side with agencies like NCMEC and law enforcement while still being able to provide end-to-end encryption and privacy to users who are not committing criminal acts shouldn't even be a question.*
>
> *Children's lives and futures are in your hands.*
>
> – Survivor

https://www.missingkids.org/theissues/end-to-end-encryption

Built largely in just the past 25 years, the digital world has developed rapidly, and continues to grow. This constantly churning sea of change leaves many parents, political leaders, judges and even law enforcement playing catch up to understand how technology is bringing offenders together with one another, as well as how technology creates both opportunities and risks for children. Furthermore, society struggles to balance its desire for innovations or policies developed for privacy, such as encryption, anonymization, and data retention, with that of safety, particularly child safety. Within this backdrop, technology-based issues frequently frustrate the collective ability to combat online child exploitation.

For law enforcement, technology, of course, is a double-edged sword, which creates both challenges and opportunities as a tool to combat child exploitation. In the arena of digital forensics, the development of protocols and tools for digital analysis in child exploitation cases is complicated by the ever-changing variety of platforms used to commit offenses, the sheer volume of data to analyze, and the cost, time, and expertise involved in development.

Given a variety of technological changes on several fronts, a perfect storm is brewing that sharply curtails law enforcement's ability to detect and investigate technology-facilitated child sexual exploitation offenses. This chapter will discuss several of the primary technological threats hindering the prevention and interdiction of child exploitation.

Increased Availability of Default Encryption

Data at Rest: The Spread of Default, Full Disk Encryption

Types of Encryption
Encryption is a technology that protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people. Full disk encryption uses disk encryption software or hardware to encrypt every bit of data, including all files and programs, that goes on a disk, device, or hard drive. End-to-End encryption is a method of secure communication that only allows the users communicating with one another to read and view the content and prevents third parties from accessing any of the data.

As a technology, encryption is not new. Nor is it inherently harmful. At the Department of Justice, we rely on encryption every day to keep sensitive intelligence and investigative information safe, and in our personal lives we benefit from the privacy afforded by encryption. At the same time, the investigation and prosecution of crime are thwarted when we cannot access the contents of a hard drive or a smart phone, even with a lawful court order or search warrant issued only after a neutral judge has determined there is probable cause that the hard drive or phone contains evidence of a crime. This impact is felt throughout the case, from identification and investigation, to charging, plea negotiations, sentencing, and restitution. Most significantly, victim identification and rescue are rendered impossible even if it is known that images or videos that could lead to that rescue reside on the device. Over the last five years, full disk encryption has become the default model of many digital devices, particularly smartphones and tablets, requiring no action by the user to obtain that warrant-proof technology. Complicating the issue is the existence of multiple types of full disk encryption, each requiring a different investigative method and/or forensic approach, and even different types of legal process. Often one case can involve multiple forms of encryption, which strains or exceeds the capacity of law enforcement's already limited forensic resources.

Data in Motion: The Spread of End-to-End Encryption (E2EE)

Many technology companies have adopted, or are adopting, end-to-end encryption (E2EE), which secures online data but also has potentially dire consequences. E2EE prevents companies or any third-party, such as law enforcement agencies with appropriate warrants or court orders, from detecting or gathering information about the activity of people who use the internet to exploit children and share CSAM. This results in countless incidents of online child sexual exploitation remaining hidden and victims going unidentified and awaiting rescue.

Nothing demonstrates the impact of the spread of E2EE more dramatically than data about the impact of Meta's[1] planned adoption of E2EE on its Messenger platform. Meta (formerly The Facebook Company) is the undisputed global leader when it comes to voluntary efforts to detect CSAM on its platforms. In 2019 and 2020, Meta-owned platforms, including Facebook, Instagram, and WhatsApp, accounted for approximately 94% of all CyberTips sent in by

[1] The Facebook Company changed its company name to Meta on October 28, 2021 https://about.fb.com/news/2021/10/facebook-company-is-now-meta/

industry each year.[2] However, The National Center for Missing & Exploited Children (NCMEC) estimates that approximately 12 million CyberTips will be lost to the implementation of E2EE on Facebook's Messenger platform.[3] Meta promises that it is developing alternative tools to detect CSAM even with E2EE, but thus far has provided no information to confirm the viability or accuracy of this claim.[4]

"If Facebook moves forward with the plans that they have at the moment, we will be blinded. They will blind themselves and law enforcement."

FBI Director Christopher Wray

Meta's data also sheds light on how much child exploitation activity must already be occurring in the dark, protected spaces of apps that already use E2EE - if this much crime is happening in the open, how much is going on where it cannot be detected? Anecdotal cases involving encrypted messaging apps like Telegram, Wickr, and WhatsApp provide a small glimpse - a tip of the iceberg - into crimes against children on encrypted platforms.[5] Beyond what these cases can tell us, we do not have a statistical picture of the prevalence and severity of child exploitation that takes place behind encryption. In the words of FBI Director Christopher Wray, "If Facebook moves forward with the plans that they have at the moment, we will be blinded. They will blind themselves and law enforcement."[6]

In this regard, E2EE poses the gravest threat to children, particularly on platforms where children are allowed to use or even encouraged to use such apps alongside adults. In these unsafe online spaces, children are easy prey for predators because voluntary detection and interdiction is impossible. E2EE blinds us all, at the expense of children.

Increased Availability of Anonymizing Technology

Anonymizing technology comes in many forms, but the core feature is that it is designed to conceal information about a user's identity and physical location. Law enforcement can watch crimes occur in real time in anonymous spaces but have no ability to identify the location of the sites or find and apprehend the offenders who access them.

The Dark Web

The Dark Web, also known as the Dark Net, is a heavily encrypted layer of the internet. Unlike the "surface web," which is the portion of the internet indexed by search engines and used by most consumers for most mainstream services, the Dark Web is designed for anonymity. Users

[2] 15,884,511 of 16,836,694 CyberTips in 2019, and 20,307,216 of 21,447,786 in 2020. Because NCMEC combines report totals for related platforms and companies, the number of CyberTips reported by Facebook includes reporting from other Meta-owned platforms, including Instagram and WhatsApp.
[3] https://www.justice.gov/opa/press-release/file/1207081/download. Pg. 2
[4] https://www.nytimes.com/2020/02/05/technology/facebook-encryption-child-exploitation.html
[5] https://www.justice.gov/usao-edva/pr/sex-traffickers-sentenced-combined-81-years-prison
https://www.texarkanagazette.com/news/texarkana/story/2020/nov/14/man-gets-17-years-prison-charges-child-pornography/849054/
https://www.justice.gov/usao-ne/pr/lincoln-man-receives-100-year-sentence-producing-child-pornography
[6] Taken from testimony in front of the Judiciary Committee of the U.S. House of Representatives on February 5, 2020.

need special software to access the Dark Web. The advanced anonymity of Dark Web platforms makes it exceptionally hard for law enforcement to identify the physical location of Dark Web sites (hence the Dark Web name for websites - "Hidden Services") and the individuals behind the illegal activity. Society has effectively created a lawless environment where a vast amount of criminal activity occurs and is tolerated under the banner of digital privacy. Although the design of the Dark Web makes it difficult to comprehensively document the staggering scope and breadth of crime occurring, some estimates indicate that 57% of the websites on the Dark Web are designed to facilitate illicit activity, with new sites being continually added.[7]

In 2018, 2.88 million accounts were registered globally across the ten most harmful child sexual exploitation sites on the Dark Web.

The Dark Web has given offenders easier, more secure access to vulnerable children and allowed people who share a sexual interest in children to build global networks and communities to discuss their predilections, share CSAM, and hone techniques to avoid law enforcement detection. In 2018, 2.88 million accounts were registered globally across the ten most harmful child sexual exploitation sites on the Dark Web.[8] One image that was posted on a Tor hidden hosting service for 24 hours was viewed 21,000 times.[9] Not only is the Dark Web attractive to more technologically sophisticated offenders who are looking to use extra measures to attempt to evade detection, but the increasing size and accessibility of Dark Web platforms has made it easier for even less sophisticated offenders to achieve heightened anonymity. Most Dark Web child exploitation communities are open forums or chat sites, which instantly connect offenders of varying degrees of sophistication. Some sites require users to pay a fee to gain access, generally using cryptocurrency payments, commercializing the abuse suffered by victims whose images are trafficked. Others require new or prospective members to provide newly produced CSAM, pushing offenders even further into their abuse of children. This amplification effect is endemic of the Dark Web, as offenders feel freer to discuss their sexual interests with others and share more niche or extreme images in the haven of these anonymized sites. These communities provide a forum for offenders to bond with one another, share stories about their past, and often go beyond just viewing and trading images to collaboratively targeting children to extort more CSAM or to gain face-to-face access to children they otherwise would never encounter.[10]

Investigations on the Dark Web often depend on innovation in strategy and law enforcement tools. Empowering law enforcement to collaborate beyond jurisdictions or national borders is a key to success in identifying victims who are broadcast on the dark web from a hidden location. While the Department of Justice has made significant success in taking on criminals utilizing the Dark Web, there is no question that such investigations are slow, inefficient, and resource intensive.

---

[7] Goodison, Sean E., Dulani Woods, Jeremy D. Barnum, Adam R. Kemerer, and Brian A. Jackson, Identifying Law Enforcement Needs for Conducting Criminal Investigations Involving Evidence on the Dark Web. Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/research_reports/RR2704.html.

[8] 'The Internet is Overrun with Images of Child Sexual Abuse. What Went Wrong?' (New York Times, 2019) available at https://www.nytimes.com/interactive/2019/09/28/ us/child-sex-abuse.html

[9] Based on investigatory and prosecutorial experience of the authors.

[10] Based on investigatory and prosecutorial experience of the authors.

Key Definitions

The Dark Web
The Dark Web is a layer of the internet that can only be accessed through special software, such as anonymous browser networks like Tor, which shields users' identities and locations. Most of the Dark Web's content is hosted anonymously.

Tor
The Onion Router (now known by its acronym Tor) is a free software that encrypts and anonymizes a user's internet activity by sending internet traffic across numerous servers to shield the user's true location. It was created as part of a federal government research project – and is still largely funded by federal agencies – but now is an open-source software available for any user.

Virtual Private Network (VPN)
A virtual private network encrypts the connection between a device and the internet to protect sensitive data being transmitted over the network. It works by masking a user's IP address, preventing unauthorized people from eavesdropping on a user's internet traffic. This technology is used widely in corporate settings to enable secure remote work by an organization's employees.

Peer-to-Peer (P2P) File Sharing Network
A peer-to-peer file sharing network acts as a decentralized repository of content, where a community of users can upload and download digital files, such as videos, software, or images.

Increase in Use and Availability of Virtual Private Networks (VPNs)

Virtual Private Networks (VPNs), like encryption, are not new, but their pervasiveness and accessibility have continued to expand. VPNs thwart the use of traditional means to identify and locate a potential suspect by encrypting the connection between a device and the internet and masking the user's IP address. Many VPNs are hosted outside of the United States, making an IP address appear to be in a particular location, when the VPN hosting service's users are active all over the world. Even when law enforcement and partner agencies identify an initial IP address for a child exploitation offender, VPN technology may result in CyberTips and leads being incorrectly routed to the service hosting country, creating a delay in getting the lead to the right local authorities in the offender's jurisdiction. Worse, the VPN may not retain real location data for its users, making the lead useless. Historically the VPN would degrade a user's download speeds, so investigators could attempt to find information on the computer when the VPN was not logged in. However, it is becoming increasingly common to require a VPN to even access the internet, so that opportunity is now generally lost.

Inability to Recover Information from Apps and Software

Smartphones are the perfect tool to sexually exploit a child as they can readily produce, trade, and store CSAM on a fully encrypted, often warrant-proof, device. In addition, users can instantly access images remotely stored, record and upload video or photographs in seconds,

initiate or receive videocalls or livestreaming, and communicate by text, email, or countless apps. Smart phones connect to social media platforms where adult offenders comingle with unwitting underage users. Offenders can also connect with likeminded offenders on a variety of platforms without limits - 24 hours a day, 7 days a week. As they become increasingly affordable with a broad global footprint, more people, particularly children, have access to smart phones and tablets than computers. In fact, over half of children in the United States have their own smartphone by age 11.[11] This allows offenders easy access to a wider socio-economic range of victims.

The ubiquity of smart phones has ushered in a corresponding increase in the use of apps, and a decrease in the use of software installed on a computer. This shift has impacted law enforcement's ability to obtain and analyze evidence to further an investigation. Investigations today may involve an offender in one country, victims in several others, and evidence (sitting on cloud-based storage systems) in even more. In addition, each app likely has its own data retention policy and its own unique data formats that may be indecipherable to law enforcement. If the app is foreign-based or stores its data overseas, it may require a Mutual Legal Assistance Treaty (MLAT) request, or foreign law enforcement engagement, to access despite the fact the data is accessed by the user in the U.S. On one device, you might have 5-10 different apps involving multiple jurisdictions. This complex international issue greatly frustrates law enforcement's ability to investigate and obtain crucial evidence even in a relatively straightforward case. When there are indicators that a child is at risk, the situation becomes urgent and outcomes potentially dire.

At the same time, many apps have short or non-existent data retention policies, which are a discretionary decision of each company, leave law enforcement with little room for delay in initiating a legal process. Data retention, or the lack thereof, is one of the biggest barriers to the successful identification of a potential offender. Apps also vary in their responsiveness to non-disclosure orders and preservation requests, causing law enforcement to spend significant effort just to make sure the offender is not tipped off and able to destroy evidence.

Technology Systemically Helping Offenders Evade Law Enforcement

Offenders are deploying a variety of measures to shield themselves from law enforcement's reach. Consider ProtonMail[12], which according to its website, is the world's largest encrypted email provider. ProtonMail stores all its data in Switzerland and 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*

[11] https://www.npr.org/2019/10/31/774838891/its-a-smartphone-life-more-than-half-of-u-s-children-now-have-one
[12] *See* https://protonmail.com/

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.

In pursuit of protecting privacy and freedom of expression, companies such as ProtonMail advertise their services in a way that unavoidably attracts individuals looking to commit crimes, including child exploitation offenders, 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.[13] Inexplicably, ProtonMail is listed with an age rating of 4+ in the Apple Appstore, which states the app contains no objectionable material and is apparently appropriate for children. Barter was only apprehended because he conversed with an undercover law enforcement officer.

Another threat to online child safety comes from technology providers who frustrate government's lawful access to information by designing themselves to essentially be sovereignless - meaning they are beyond the reach of legal requests for information from **any** country. For example, Telegram is an encrypted cloud-based mobile and desktop messaging app that purposefully stores data in multiple jurisdictions around the globe so that law enforcement must obtain several court orders from different jurisdictions to obtain any useable information.[14] 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."[15]

Non-responsive File and Image Hosting Services (Bulletproof Hosting)

Bulletproof hosting services are file and image-sharing platforms with little to no restrictions regarding what kind of content can be hosted on their site, that do not, and are not required to, cooperate with law enforcement.

Offenders often prefer to use "bulletproof hosting" sites to share files and images with one another. Bulletproof hosting sites operate in largely the same way that other web-based file sharing platforms do, but take a much more lenient, "don't ask, don't tell" stance concerning what kind of content can be hosted on their platform. They also ignore requests or fail to remove illicit content from their sites. Often, these file hosting platforms are based outside of the United States in countries with less stringent or non-existent content removal requirements and practices, making such platforms attractive to offenders wishing to evade law enforcement. This is a prolific problem that often thwarts domestic investigations.

[13] *See* https://www.justice.gov/usao-edtx/pr/dark-web-cannibal-sentenced-40-years-followed-lifetime-supervised-release.
[14] *See* https://telegram.org/faq#q-do-you-process-data-requests
[15] *See* https://telegram.org/faq#q-do-you-process-data-requests.

These services operate as the delivery mechanism for offenders sharing CSAM with one another. Offenders will post previews of CSAM on the Dark Web sites noted above, but the full photo or video is hosted on separate storage websites that are outside the United States. Other users must download the media, generating new copies of the files on their computers. This means that, even if the CSAM image or video is removed from the hosting site, several other privately held copies likely exist, which may re-emerge on the internet at any time.

Offenders also share tips with one another about which file sharing sites have poor or nonexistent monitoring and removal practices, resulting in a massive concentration of content on these sites. On any given day, there may be more than 2,000 postings on Dark Web sites linking to bulletproof hosting websites where a file containing CSAM is stored.[16]

Free.FR
Free.fr is a "bulletproof hosting" service based in France. Many offenders have used Free to anonymously store and distribute CSAM online. In 2021, the Canadian Centre for Child Protection released a report estimating that more than 2.7 million CSAM images or video media files have appeared on Free's hosting service.[17] The service is popular for its ease and scale. Users do not need to register or make an account to begin using the service, and no contact or payment information is required to start sharing files. Free provides a very generous file size limit, allowing for large media collections to be uploaded and distributed. It also offers password protection for files, limiting who can access the content, further shielding content from detection.

Use of Multiple Platforms

Offenders who use multiple platforms, or more precisely, identify and groom children on one platform, and then convince them to switch to a different platform that offers less protection for children, are a significant challenge for both law enforcement and industry. For law enforcement, the digital trail can go cold when this happens, or in the alternative, it can lead to duplication of effort because it is difficult to de-conflict investigations conducted by different agencies on different platforms that involve the same target. For the tech industry, this is a great limitation on child safety. One platform can have industry-leading child protection measures, but those mean little if a child is lured away from that protected online space into one where they are on their own.

Other Ways Offenders Use Technology

Some offenders are learning to use technology in anticipation of defending themselves from criminal charges. For example, offenders may leave their wireless router publicly available to set up a defense that someone else may have been the perpetrator. Similarly, certain apps are designed to hide themselves as a storage container on a mobile device. Thus, it appears to be one type of app (music oriented) but in fact, it is basic storage that can be used to store CSAM.

[16] Based on the investigatory and prosecutorial experience of the authors.
[17] Project Arachnid: Online Availability of Child Sexual Abuse Material, The Canadian Centre for Child Protection, June 8, 2021 https://protectchildren.ca/pdfs/C3P_ProjectArachnidReport_en.pdf

Case Example
A Fresno, California, man pleaded guilty to five counts of production of child pornography, as well as one count of receipt of child pornography, in May of 2020. The defendant's activities initially came to light in 2017, when the parents of a then six-year-old discovered that the minor had communicated with and created sexually explicit images at the request of another user on the social media application Musical.ly, now known as TikTok. A search of the defendant's digital media revealed that he had successfully persuaded and coerced multiple minors to produce sexually explicit material by pretending to be a modeling agent or to be a minor himself. He used Snapchat, Kik, Musical.ly and other applications to communicate with at least 50 minors.[18]

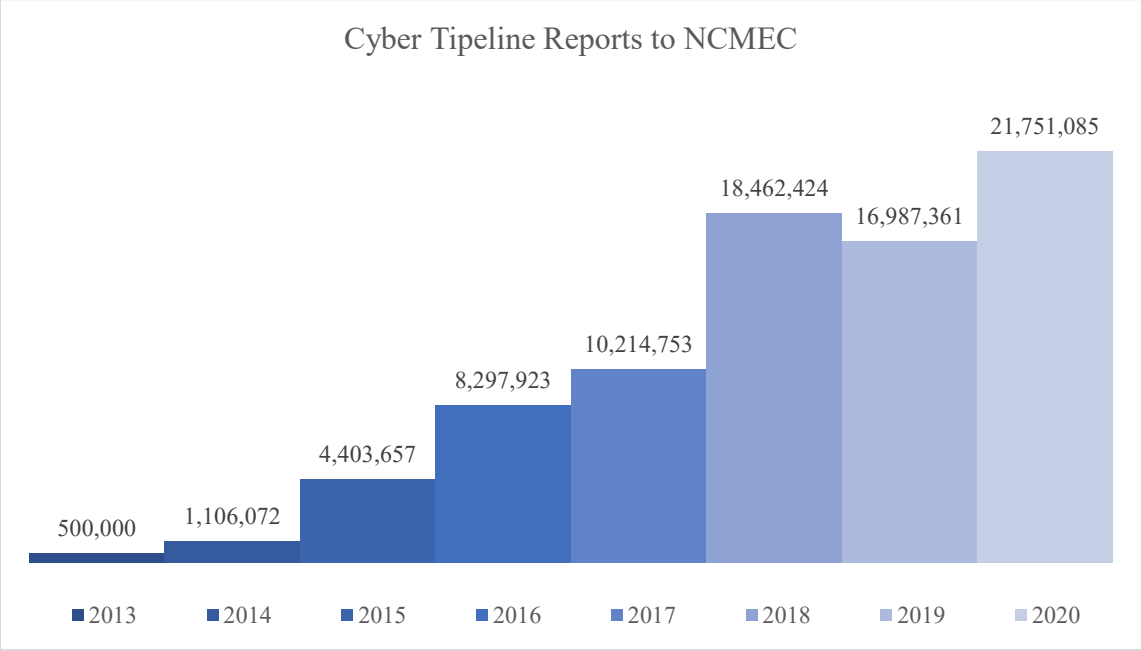
CyberTip Volume

NCMEC's CyberTipline is the United States' centralized reporting system for the online exploitation of children. The public and electronic service providers can make reports of suspected online enticement of children for sexual acts, child sexual molestation, CSAM, extraterritorial child sexual abuse (sometimes misleadingly referred to as child sex tourism), child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, and misleading words or digital images on the internet. NCMEC uses staff and automated systems to review each tip and work to determine if a child is in imminent risk, as well as determine a potential location for the incident reported so that it may be made available to the appropriate law-enforcement agency for possible investigation. By statutory mandate, U.S.-based Electronic Service Providers (ESPs) that locate CSAM on their platforms must report such incidents to NCMEC which, in turn, makes these reports, numbering in the thousands to millions, available to law enforcement in nearly every country on the planet. ESPs are not required to scan content for CSAM but if they voluntarily take affirmative steps to locate it or it otherwise comes to the ESPs' attention, they are required by federal law to report it to NCMEC.

From 2013 to 2020, the number of CyberTips sent to NCMEC skyrocketed from 500,000 to almost 22 million. On three occasions in this period, the volume of CyberTips doubled or nearly doubled from one year to the next; in 2014 the number of CyberTips was four times greater than the prior year. In 2020, the 22 million CyberTips sent to NCMEC constituted an overall increase of approximately 28% from the 2019 total.[19,20] In 2021, reports again increased to over 29.3 million, a 35% increase from 2020.[21] Though the majority of CyberTips are forwarded to overseas law enforcement, hundreds of thousands of CyberTips are sent to U.S. law enforcement every year. The Internet Crimes Against Children (ICAC) Task Forces, a national network of 61 coordinated task forces across federal, state, and local law enforcement and prosecutorial

[18] https://www.justice.gov/usao-edca/pr/fresno-man-admits-sexual-exploitation-least-50-children-through-multiple-social-media
[19] *See* https://www.missingkids.org/gethelpnow/cybertipline#bythenumbers.
[20] Although the CyberTipline is a mechanism for American companies to report online child exploitation, we must emphasize that year over year, the majority of CyberTips (typically around 90% of reports received per year) are forwarded to law enforcement in foreign countries.
[21] *See* https://www.missingkids.org/gethelpnow/cybertipline

agencies, are the primary receiving investigative entities for Cybertips. Since 2016, ICACs have investigated more than 1 million CyberTips.[22] with each year bringing a relative percentage increase similar to the overall increase in CyberTips.



It is helpful that some companies still can detect CSAM on their platforms and are voluntarily doing so. The increases in CyberTips in recent years can likely be attributed to three factors: the growth of the overall number of users of online platforms, the creation and use of PhotoDNA hash sets, and the use of these hash-based monitoring systems by large online platforms including Facebook, Google, and Microsoft. PhotoDNA is an image-identification technology that creates a unique digital signature (known as a "hash") to represent each image, which can then be used to identify other instances of the image (matching hashes), even if the image has been recolored or resized.[23] The technology allows online service providers to detect, report, and remove child sexual abuse images shared on their sites, and the collective database of the images that have been found to date allows law enforcement to prioritize investigations into newly produced CSAM.

The deluge of actionable CyberTips could disappear tomorrow if more and more providers implement E2EE, blinding providers to additional parts of the digital world. While the tips would decrease, the exploitation of children would undoubtedly continue – unabated and undetected. In the meantime, however, the volume and the quality of CyberTips remains a challenge for law enforcement as they attempt to discern the signal from the noise to prioritize which tips to investigate first. Some small changes would provide outsize benefits, such as making it easier for NCMEC to package together individual CyberTips involving the same offender for law enforcement, even if they were received on different dates or involve different platforms. Implementing a good feedback loop between law enforcement and the tech industry could also

[22] *See* Internet Crimes Against Children (ICAC) Task Forces Review appendix.
[23] https://www.microsoft.com/en-us/photodna

help make the CyberTip system more effective, such as by eliminating repeated CyberTips involving the same content that is not actionable. Such communication is hampered because some in the tech industry feel that the Stored Communication Act,[24] which bars online providers from disclosing additional content or communicating with law enforcement except in response to legal process, limits its ability to share information or evidence it inadvertently encounters running its platforms.[25]

Co-mingled Adult and Child Platform Users

The popularity of social media and online gaming platforms cannot be overstated. They have fundamentally changed the way people live their lives. Posting your story online, filming a dance video, or building an online world with friends have become synonymous with adolescence today. However, these activities are not the exclusive province of global kids and teens. Adults similarly orient their lives today around online communities, gaming platforms, and information sharing. Thus, the worlds of kids and adults intersect online in ways that are deemed unacceptable and discouraged in the physical world. Adults have unsupervised and largely unfettered access to children online not just in their own communities, but across the world. They can chat with children, pretend to be children themselves, and quietly stalk and develop relationships with dozens of children simultaneously. Unfortunately, even if they have stated age restrictions, providers do little to verify the ages of their users or keep children separated from adults online. The result can be catastrophic for an unsuspecting child who falls prey to the seasoned online predator.

Maintaining Capacity at the Front Line

Building and maintaining expertise in the investigation and prosecution of online child exploitation offenses has always been a challenge. That has never been truer than in 2020 and 2021 when law enforcement was stretched thin by the demands of the pandemic response. We anticipate that post-pandemic data will show high rates of retirement from law enforcement, and a low rate of recruitment, which will reduce the overall experience level of the police force. At the same time, specialized expertise is needed more than ever to respond to the onslaught of technological and resource challenges, which include the following:

Increased Investigative Costs

Routine investigative steps are expensive. For example, Google and other online providers can charge a substantial fee to respond to legal process.[26]

In addition, forensic tools and certifications not only need to be obtained, but maintained, which again requires capital. Building effective password cracking mechanisms, for example, takes significant time and money. Further, there are costs associated with running and updating forensic tools, training personnel on the updates, and so on. Tools can quickly become outdated

[24] 18 U.S.C. § 2701 to 2710 https://www.justice.gov/archives/jm/criminal-resource-manual-1061-unlawful-access-stored-communications-18-usc-2701
[25] *See* additional discussion on *U.S. v. Wilson* in the Unique Resource and Enforcement chapter.
[26] Based on the investigatory and prosecutorial experience of the authors.

with updates and changes from device makers like Apple and Google. Ironically, even if an agency can cover the cost to obtain data from an online provider and have forensic or analytical capacity for review, the data itself may come in a proprietary format unique to the online service that is unrecognizable to known forensic tools, leaving agencies with a large bill and no results.

These investigative costs create a disparity among different socio-economic communities. Well-funded police departments in wealthy areas are more likely to have the ability to solve cases than departments in poorer areas. Smaller agencies might struggle to meet these costs and choose to either withdraw a legal request or never submit it at all.

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 over the past 5-10 years with gigabytes of stored data becoming terabytes. In addition, the volume of devices, many containing little to no evidence, located during searches has 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 evidence, 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 (*see* RCFL table below), 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 (*see* ICAC table below). 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.[27]

[27] 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.

RCFL Child Exploitation Cases by Year (FY2016-FY2021)

RCFL Child Exploitation Cases[28]						
Office	**FY2016**	**FY2017**	**FY2018**	**FY2019**	**FY2020**	**FY2021**
CGRCFL	808	877	960	1,444	1,055	1,565
GHRCFL	270	297	329	374	351	451
HARCFL	468	439	640	741	638	627
IWRCFL	388	387	405	429	466	599
KRCFL	149	163	195	217	179	368
NERCFL	--	2	131	226	359	623
NJRCFL	352	353	299	250	321	723
NMRCFL	306	279	264	273	267	369
NTRCFL	480	477	450	570	489	489
NWRCFL	187	167	198	262	279	300
OCRCFL	684	617	714	900	680	1010
PHRCFL	529	496	446	578	596	748
RMRCFL	186	201	227	489	555	558
SDRCFL	532	543	484	550	479	814
SVRCFL	331	357	366	400	316	294
TVRCFL	--	28	25	404	325	323
WNYRCFL	187	160	176	180	253	429
TOTAL	**5,857**	**5,843**	**6,309**	**8,287**	**7,608**	**10,290**

ICAC Computer Forensic Exams by Year (FY2016-FY2021)

ICAC Computer Forensic Exams[29]							
State	**Task Force Agency**	**FY2016**	**FY2017**	**FY2018**	**FY2019**	**FY2020**	**FY2021**
AK	Anchorage Police Department	651	351	442	389	269	276
AL	Alabama Law Enforcement Agency	418	652	1,749	449	1,024	1,290
AR	Arkansas State Police	1,867	1,418	1,478	1,408	1,287	1,406
AZ	Phoenix Police Department	1,249	2,221	2,422	2,403	2,838	2,666
CA	Los Angeles Police Department	1,822	1,663	2,753	1,233	2,512	4,984
CA	San Diego Police Department	621	744	900	467	373	551
CA	San Jose Police Department	768	880	873	2,794	2,964	2,551

[28] This data was pulled from the CART Database Case Management System. The accuracy of these numbers cannot be verified as the database only contains and reports on what was entered into the system by various users.
[29] *See* Internet Crimes Against Children (ICAC) Task Forces Review appendix.

CA	Fresno County Sheriff's Office	421	485	480	507	724	632
CA	Sacramento County Sheriff's Office	911	1,072	704	708	863	1,080
CO	Colorado Springs Police Department	1,140	1,283	1,378	1,281	1,108	1,392
CT	Connecticut State Police	896	680	923	482	285	219
DE	Delaware Department of Justice	372	278	194	135	46	104
FL	Broward County Sheriff Office	991	1,080	1,206	1,498	1,691	1,573
FL	Gainesville Police Department	1,988	1,589	1,967	1,581	2,413	2,059
FL	Osceola County Sheriff's Office (Polk County Sheriff's Office for FY16 and FY17)	2,897	2,677	1,067	2,091	2,697	2,466
GA	Georgia Bureau of Investigation	1,678	2,039	2,038	2,225	1,844	2,475
HI	Hawaii Department of the Attorney General	9	8	114	76	147	200
IA	Iowa Division of Criminal Investigation	868	812	800	1,308	1,033	1,159
ID	Idaho Office of the Attorney General	863	240	276	371	463	536
IL	Cook County State's Attorney's Office	369	251	307	335	258	265
IL	Illinois Office of the Attorney General	1,456	1,824	1,186	1,288	1,407	1,338
IN	Indiana State Police	1,861	2,523	2,227	2,558	2,259	2,633
KS	Sedgwick County Sheriff's Department	634	663	704	697	658	895
KY	Kentucky State Police	919	672	649	855	818	845
LA	Louisiana Department of Justice	973	1,171	956	1,043	721	712
MA	Massachusetts State Police	1,179	1,338	1,440	1,675	509	380
MD	Maryland State Police	944	1,065	1,049	1,118	1,432	1,624
ME	Maine State Police	587	289	400	534	584	448
MI	Michigan State Police	232	5,728	8,359	8,028	7,324	7,278
MN	Minnesota Department of Public Safety	1,379	1,856	1,865	1,733	1,577	1,396
MO	St. Charles County Sheriff's Department	3,685	3,703	3,352	3,025	2,861	2,427

MS	Mississippi Office of the Attorney General	771	861	691	678	796	757
MT	Montana Department of Justice - Division of Criminal Investigation (Billings Police Department for FY16 and FY17)	382	198	415	426	314	193
NC	North Carolina State Bureau of Investigation	1,694	4,093	2,339	1,863	2,637	2,302
ND	North Dakota Office of the Attorney General	390	592	566	669	759	771
NE	Nebraska State Patrol	1,534	1,276	1,171	607	678	701
NH	Portsmouth Police Department	736	676	716	1,218	1,375	1,233
NJ	New Jersey Department of Law and Public Safety	2,943	3,124	3,327	4,801	3,356	2,366
NM	New Mexico Office of the Attorney General	962	812	964	812	617	687
NV	Las Vegas Metropolitan Police Department	1,251	1,101	995	956	971	945
NY	New York City Police Department	245	386	380	329	200	237
NY	New York State Police	2,790	2,647	2,635	2,944	3,662	2,681
OH	Cuyahoga County Prosecutor's Office	1,951	1,419	1,234	1,249	1,921	1,940
OK	Oklahoma State Bureau of Investigation	294	484	1,361	720	593	813
OR	Oregon Department of Justice	102	87	296	498	426	362
PA	Delaware County District Attorney's Office	5,434	4,196	3,875	4,566	2,873	3,641
RI	Rhode Island State Police	221	340	465	371	408	288
SC	South Carolina Attorney General's Office	776	720	1,457	1,440	786	1,409
SD	South Dakota Office of the Attorney General	1,160	1,485	1,142	1,167	1,141	1,061
TN	Knoxville Police Department	1,604	1,684	2,333	1,872	1,903	1,771
TX	Houston Police Department	1,100	952	703	627	850	911

TX	Dallas Police Department	725	1,725	982	1,159	1,490	1,711
TX	Office of the Attorney General of Texas	1,608	2,397	1,383	1,259	1,700	2,251
UT	Utah Office of the Attorney General	2,364	1,759	2,089	1,741	1,559	1,544
VA	Bedford County Sheriff's Office	1,400	1,866	1,882	1,909	1,604	1,709
VA	Virginia State Police	3,895	1,464	1,389	1,265	1,151	1,152
VT	Vermont Office of the Attorney General	325	339	336	249	211	241
WA	Seattle Police Department	585	831	1,003	821	897	3,611
WI	Wisconsin Department of Justice	3,393	4,351	4,649	4,522	4,644	3,907
WV	West Virginia State Police	1,582	1,443	1,222	1,369	1,046	1,151
WY	Wyoming Office of the Attorney General	336	321	217	110	136	112
TOTALS		**77,201**	**84,884**	**86,475**	**86,512**	**85,693**	**90,318**

Deficient Analysis

Deficiencies in forensic capacity do not just center on volume. Dramatic variations in quality of the forensic processing also pose a substantial challenge. This variation largely stems from a "generalist" approach to forensic examination, rather than a more collaborative, nuanced investigation. Often, forensic investigators simply focus on data extraction, then hand the investigation off to an agent to conduct the evidence review.

The problem with this approach is two-fold. First, the computer forensic examiners may not extract all the relevant evidence, focusing on the image files alone. For example, the examiner may not understand the significance of the file structure, chat applications, browsing history, or other indicators that could signal a more dangerous offender. Second, the agent tasked with the review of digital evidence may lack the experience to be able to render or efficiently review the data. There are few, if any, standard protocols for forensic examinations specifically in child exploitations. As a result, information/evidence from different sources (such as cloud storage, home devices, and mobile devices) may not be married up effectively in a way that allows law enforcement to take appropriate action. Additionally, without adequate computer forensic expertise among law enforcement agents, important insight and detail will be lacking when designing and implementing proactive investigations that target entire platforms or websites.

Because online child exploitation offenders often engage in similar patterns of activity, it is more useful to obtain computer forensic analysis from examiners who possess some subject matter expertise with online crimes against children. Knowing the preferred platforms, offender methods, and how seized data intersects with cloud-based data is crucial. The need for trained

specialized computer examiners who are familiar with child exploitation offenders has never been greater.

Expertise on the Execution of Search Warrants

When executing a search warrant for digital media, law enforcement needs training and guidance on how to handle any number of issues, including legal and technical solutions to biometric locks on digital devices (such as using a fingerprint or facial recognition to unlock a device), and how to time the execution of the warrant to maximize the amount of data that will be available for seizure. The success of an investigation often depends on the training of forensic and investigative personnel at the search warrant scene, and the communication among them, so that they know what to look for, what to ask for, and how to conduct an effective interview if the target agrees to one. Personnel must know how to identify different types of encryptions, how to tailor their approach accordingly and must know when devices will lock down or erase. As law enforcement strives to keep up with emerging technologies and platforms, they cannot forget how to handle older technologies. Indeed, new forensic tools are only looking for evidence based on today's technology, even though some offenders continue to use older technologies.

The issues with the execution of a search warrant can be so complicated that additional personnel are needed. For example, addressing encryption on scene is very time consuming, and may continue many hours after the evidence has been seized. Forensic examiners are needed to supplement automated tools.

For example, if a tool is missing data, the examiner will have to go back and figure out how to find what was missed. Of course, some jurisdictions do not have forensic personnel available to assist on scene during search warrants, and often, those on scene have not received sufficient training to address the issue of encryption.

Officer Safety

The tragic murders of FBI Special Agents Dan Alfin and Laura Schwartzenberger, and injury of three other agents, in February of 2021 during the execution of a CSAM-related search warrant underscores the incredible danger law enforcement can face when approaching targets, particularly those who use technology such as smart doorbells, which lets them see the agents coming.[30] This risk can be particularly acute when investigating crimes against children, because the stress offenders may feel at being exposed may cause them to act in a dangerous or erratic manner. These considerations, along with the preservation of critical evidence potentially jeopardized by encryption, must be considered when developing policy for requesting search warrant protocols for entry.

Training for Prosecutors

Training is also critical for prosecutors who handle crimes against children. The technology and platforms used by offenders to perpetrate these crimes are changing rapidly and becoming increasingly sophisticated, as are the laws in place governing these tools. Prosecutors must fully

[30] https://www.fbi.gov/news/stories/honoring-fallen-special-agents-laura-schwartzenberger-and-daniel-alfin-020821

understand digital evidence and digital forensic investigations to draft effective search warrants, make the best charging decisions, and construct compelling evidence presentations at trial. This training must include understanding how digital forensic investigations are approached, how digital evidence is used in court, challenges involved in evidence admission, and how to identify and access evidence that is critical to the government's case at sentencing. The DOJ is working to provide this training via national training events[31], as well as building connection points across the Child Exploitation and Obscenity Section[32] and other Project Safe Childhood practitioners to share expertise, resources, and best practices in this evolving area.

Additionally, prosecutors need to be provided the mental health support necessary to cope with the impact of dealing with these horrific crimes daily. The weight of this work is extreme: in addition to having to regularly view child sexual abuse in the images and videos involved in their cases, investigators and prosecutors carry the weight of a child's safety on their shoulders. This can lead to significant negative mental and physical health outcomes, and lead many to leave the field altogether, limiting the ability to apprehend offenders and prevent future offending.[33]

Need for New Investigatory & Collaboration Tools

Just as online child sexual exploitation can be exacerbated by technological advancements that favor offenders, so too can it be combatted through technological innovation. New technological tools can help the tech industry, NGOs, and investigators and prosecutors more effectively identify and interdict online crimes against children.

Need for New Forensic and Interdiction Tools

In 2009, Microsoft partnered with Dartmouth College to develop PhotoDNA, a technology that aids in finding and removing known images of child exploitation. The advent of PhotoDNA has assisted in the detection, disruption, and reporting of millions of child exploitation images. However, a tool is still needed to apply a standardized, effective hashing system to video files, as well as a tool to detect online predators attempting to lure children for sexual purposes. Natural language processing and data analytics could be deployed as possible early detection measures. Current methods of detecting livestreaming of sexual activity requires a large amount of human capital, and there remains no automated method to identify newly produced material. Finally, any new tools that are developed should focus on being able to merge different evidence streams to enable more efficient analysis and data sharing.

The development and refinement of these tools will take dedicated resources, including the creation of full-time jobs or programs devoted to doing this work. It is impractical and inefficient to expect dedicated agents with some computer science and forensics knowledge to attempt to build tools on shoe-string budgets to investigate or analyze digital platforms that have trillion-dollar market capitalization and command the best and brightest dedicated computer programmers in the world. There is also always a delay between the emergence of a new

[31] https://ojjdp.ojp.gov/national-training-and-technical-assistance-center
[32] https://www.justice.gov/criminal-ceos
[33] These issues are discussed further in the Wellness Challenges for Law Enforcement Personnel chapter.

technology and the adoption and deployment of tools to leverage that technology. We need to find ways to shorten that time delay and ensure that existing, effective approaches are not sacrificed when technology changes.

To be sure, these tools would not be a complete fix to online child sexual exploitation. However, these tools could do more than just support investigations. They could also be useful in making online environments inhospitable to CSAM, helping to rapidly remove CSAM and stop the cycle of revictimization endured by survivors. Further, they could protect victims from ongoing stalking and harassment because of their imagery remaining available to new offenders on the internet.

Information Sharing Among Law Enforcement

Over time, several different image repositories (commonly referred to as hashsets) have been developed in the United States to support investigations and identify, locate, and rescue the children depicted in CSAM imagery. One such repository is part of the Child Victim Identification Program (CVIP) at NCMEC. When a victim of CSAM is identified, law enforcement will provide notice of the identification of that child victim to NCMEC to be added to the CVIP database. Separately, when a law enforcement investigation involves CSAM, they will gather any imagery seized through that investigation and send it to NCMEC, which will compare it with imagery in the CVIP database. NCMEC then generates a report that is sent back to law enforcement advising them which files in the defendant's collection may contain children who have been previously identified. The information included in the report is used to provide victims with the rights they are entitled to under law and may help prosecutors build a criminal case.

Although the FBI and HSI can and do periodically compare and share their own image repositories with one another, neither currently does so with the CVIP repository, which also includes state and local submissions as well as distributed international images and videos. Whatever image comparison and sharing does occur is irregular and dependent on individual agents who initiate the process when time allows. This leaves law enforcement, as well as NCMEC, without the best up-to-date information as to which children have been identified and rescued, and which should be a priority to be identified and rescued. Victim identification and CSAM investigations would benefit from ensuring that all investigative entities have access to coextensive image repositories.

Staying Current

For CSAM investigative tools to remain effective, they need to have comprehensive, current datasets. This is done by constantly updating with them with new, additional CSAM content, which is expensive and time consuming. Further, it relies on sharing information regarding CSAM investigations that can be challenging when thousands of local, state, and federal law enforcement entities, each with independent policies on data sharing, have simultaneous jurisdiction over CSAM offenses. Similarly, there is a never-ending need for open communication and sharing of investigative best practices, lessons learned, and latest developments that arise in the field. Some new developments are not fully taken advantage of

because they are not shared among law enforcement. Each of these problems suggest the need for an integrated center, bringing together federal, state, and local law enforcement resources, and offering training and tools for combating child exploitation with a dedicated, innovating management team.

Technology as a Solution: Thorn

Thorn is a non-profit that builds technology to defend children from online sexual abuse. They've built several tools to aid in preventing and combating child exploitation.

Thorn's flagship product, Spotlight, is a web-based tool used by law enforcement in all 50 states and Canada to accelerate victim identification and streamline law enforcement workflows so they can respond to instances of child sex trafficking with speed. Spotlight has helped identify more than 17,000 child victims of human trafficking in the past four years and resulted in over 60% in time savings for law enforcement. They also offer a commercial product called Safer, which allows electronic service providers to identify, remove, and report CSAM on their platforms.

Lastly, Thorn runs the country's most extensive online child sexual abuse deterrence program, communicating directly with people searching for CSAM, disrupting their sense of anonymity, and encouraging them to seek help. They are constantly testing messaging, identifying the best tactics to reach and persuade specific sub-groups of offenders to seek help, and capturing aggregate data to inform future research.[34]

Offender Targeting – Working with Domestic and International Partners

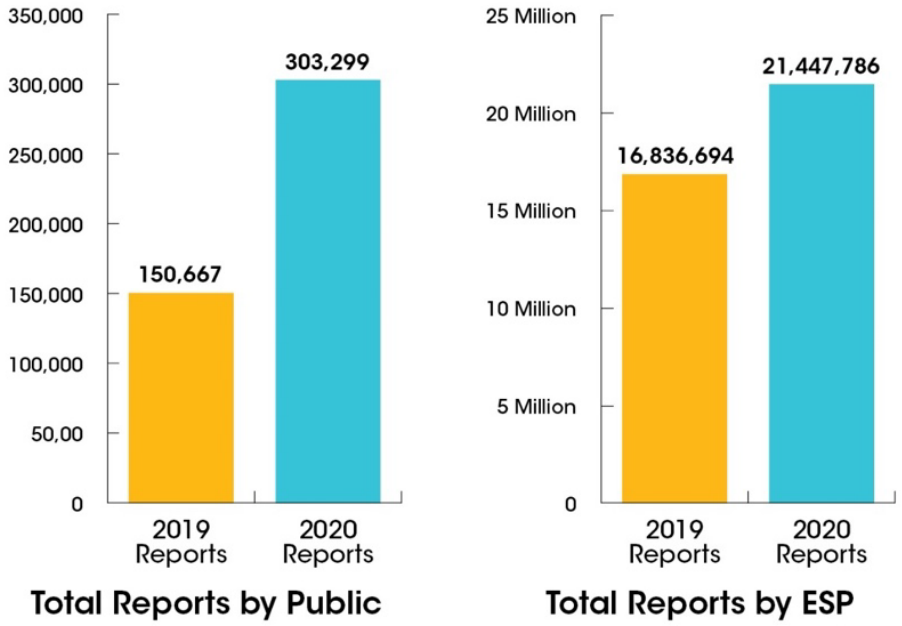
Great strides have been made in the effort to identify victims using collaborative image and video analysis. However, offender targeting is frequently siloed within investigative agency systems without the benefit of local, state, federal, or international counterparts who often are investigating the same offenders. More problematic, the evidence needed to effectively identify offenders and victims may sit within seized data that another investigative agency, even one situated only a few miles away, possesses.

This phenomenon is fueled by an online environment that frustrates traditional notions of geographic jurisdiction. For example, in Dark Web investigations, offenders and the websites they frequent lack a known location so online investigators from the world over may target them. Further, jurisdiction for child sex offenders nearly always exists across various federal, state, and local law enforcement entities. Despite this jurisdictional overlap, offender targeting is dependent on individual law enforcement priorities, resources, and capacity, and the strategic targeting, data, and analysis is fundamentally disconnected. Technology can play a critical role in building a more integrated approach.

[34] https://www.thorn.org/our-work-to-stop-child-sexual-exploitation/

Role of Industry in Online Safety

Most people have little awareness of just how pervasive CSAM is across online platforms, or the real risk children face online. Adults and children effectively navigate online highways every day that governments neither control nor regulate. Even more significant, they are also unaware of what internet-based companies are doing to protect children online, often assuming companies have built in robust practices to keep children safe and their platforms free of illicit content. The age rating system in App Stores reflects this confusion. The name "age rating" seemingly reflects an assurance of safety for a particular childhood age when nothing could be further from the truth. Sadly, there is a stark difference between perception and the reality when it comes to online safety. It is only through robust transparency regarding online safety practices, much the way we have access to automobile safety reports or other products safety mechanisms, that parents, children, and broader society at least understand the dangers of the digital world.[35]



There is no question that the tech industry plays an important role in eradicating online child sexual exploitation. The explosion in CyberTips coming from tech platforms alone demonstrates the dire need for industry engagement to make online environments inhospitable to CSAM. As noted, Microsoft led the development of a tool that has been used for well over a decade to help find CSAM, as well as one to detect online grooming. Google took the initiative to develop a *Special Victims Investigation Unit,* which focuses on more egregious CyberTips to supplement reports with more information, leading to a faster response by law enforcement. To deter queries seeking CSAM on Google's search engine, it launched an improved deterrence message for queries that appear to be seeking CSAM.

[35] Electronic Service Providers (ESP) make the majority of CyberTipline reports, but reports of online sexual exploitation from the public more than doubled in 2020. https://www.missingkids.org/gethelpnow/cybertipline

However, data suggests that there is 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, NCMEC received CyberTips from only 148 companies (approximately 10% of registered companies). The results in 2020 were barely any better, with 168 companies sending in CyberTips (approximately 12% of registered companies). Looking more closely at the data reveals the massive disparity in the effort by companies across industry. In both years, a single company—Meta—accounted for approximately 95% of all CyberTips sent in by industry that year, and three companies were the source for approximately 98% of CyberTips (Facebook, Google, and Microsoft in 2019, and Facebook, Google, and Snapchat in 2020). In contrast, in 2019 and 2020, the majority of companies that sent in any CyberTips at all (66%) each sent in less than 100 reports for the year.[36]

Similarly, a recent report released by the Canadian Centre for Child Protection (C3P) reveals the lackadaisical response by some online providers to requests to remove CSAM on their platforms, including some who take longer than 42 days to remove the material. Worse, their data shows a massive problem with "image recidivism," which occurs when imagery that had been subject to a removal notice is later reposted on the same platform: almost half (48%) of media targeted by removal notices had previously been flagged by C3P's Project Arachnid.[37]

Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse

This disparity in industry response led the Departments of Justice and Homeland Security to join ministerial counterparts from Australia, Canada, New Zealand, and the United Kingdom (collectively, the Five Eyes Countries), to develop and launch the *Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse* on March 5, 2020. Developed in consultation with representatives from six leading technology companies (Facebook, Google, Microsoft, Snap, Twitter, and Roblox), 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.[38]

The focus has now turned to gathering information from the tech industry about who has endorsed the Voluntary Principles, and how they have been implemented, particularly among members of the Technology Coalition. Formed in 2006, the Technology Coalition is comprised of 23 tech industry leaders represented by individuals who specialize in online child safety issues. All six companies who contributed to the Voluntary Principles are members of the Technology Coalition. The Tech Coalition indicates that it is committed to technological innovation to thwart online child sexual exploitation, collective action, independent research,

[36] *See* https://www.missingkids.org/content/dam/missingkids/pdfs/2019-reports-by-esp.pdf and https://www.missingkids.org/content/dam/missingkids/pdfs/2020-reports-by-esp.pdf.
[37] Project Arachnid: Online Availability of Child Sexual Abuse Material, The Canadian Centre for Child Protection, June 8, 2021 https://protectchildren.ca/pdfs/C3P_ProjectArachnidReport_en.pdf
[38] A copy of the principles is available here: https://www.justice.gov/opa/press-release/file/1256061/download.

information and knowledge sharing, and transparency and accountability.[39] In furtherance of this effort, members of the Tech Coalition published transparency reports in 2021.[40] Although company-to-company comparisons are difficult, the transparency reports do set forth measures taken by each company to combat online child sexual exploitation.

Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse

In 2020, WeProtect Global Alliance, which currently comprises 97 governments, 25 technology companies and 30 civil society organizations, committed to adopting and promoting these principles at a global level to drive collective industry action.

Principle 1: Companies seek to prevent known child sexual abuse material from being made available to users or accessible on their platforms and services, take appropriate action under their terms of service, and report to appropriate authorities.

Principle 2: Companies seek to identify and combat the dissemination of new child sexual abuse material via their platforms and services, take appropriate action under their terms of service, and report to appropriate authorities.

Principle 3: Companies seek to identify and combat preparatory child sexual exploitation and abuse activity (such as online grooming for child sexual abuse), take appropriate action under their terms of service, and report to appropriate authorities.

Principle 4: Companies seek to identify and combat advertising, recruiting, soliciting, or procuring a child for sexual exploitation or abuse, or organizing to do so, take appropriate action under their terms of service, and report to appropriate authorities.

Principle 5: Companies seek to identify and prevent child sexual exploitation and abuse facilitated or amplified by livestreaming, take appropriate action under their terms of service, and report to appropriate authorities.

Principle 6: Companies seek to prevent search results from surfacing child sexual exploitation and abuse and seek to prevent automatic suggestions for such activity and material.

Principle 7: Companies seek to adopt enhanced safety measures with the aim of protecting children, in particular from peers or adults seeking to engage in harmful sexual activity with children; such measures may include considering whether users are children.

Principle 8: Companies seek to take appropriate action, including providing reporting options, on material that may not be illegal on its face, but with appropriate context and confirmation may be connected to child sexual exploitation and abuse.

[39] https://www.technologycoalition.org/#vision.
[40] https://www.technologycoalition.org/annualreport/

Principle 9: Companies seek to take an informed global approach to combating online child sexual exploitation and abuse and to take into account the evolving threat landscape as part of their design and development processes.

Principle 10: Companies support opportunities to share relevant expertise, helpful practices, data, and tools where appropriate and feasible.

Principle 11: Companies seek to regularly publish or share meaningful data and insights on their efforts to combat child sexual exploitation and abuse.

Leveraging Tech to Improve Threat Transparency Globally

The advent of PhotoDNA has enabled two key methods of making the online environment inhospitable for CSAM. First, the widespread voluntary use of PhotoDNA has revealed a high volume of CSAM on even large, well-known sites like Facebook, Google, Microsoft, Twitter, and Snapchat. This data is captured in NCMEC CyberTips. Second, Project Arachnid combines PhotoDNA and web-crawling technology to supplement Industry's voluntary efforts by combing all parts of the web. The notices sent through Project Arachnid to companies hosting CSAM on their sites allows for those companies to act.

These methods of interdiction are encouraging and indicate the ability of private industry and civil society to stop the circulation of CSAM online. However, more could be done. For example, child protection efforts would be greatly improved if there were a hashing standard like PhotoDNA that worked for videos, if there were a well-vetted, collaborative hash sharing database easily accessed by all Industry members, and if there were robust efforts by private industry and civil society to support web-crawling efforts like Project Arachnid.

Unfortunately, these measures are still only a beginning. There is a wealth of information available that can inform our collective understanding of the online risks. It will require focused effort and dedicated resource allocation for political and industry leadership to fully understand and address the risk posed to children online.

Strategic Response

Short-Term Goals	Long-Term Goals
Continued engagement with the tech industry on the Voluntary Principles, emphasizing the need for transparency on how the Principles are implemented, and the importance of robust child safety measures in spaces where adults and children are co-mingled.	Expand forensic capacity to obtain and analyze evidence on digital devices and in the cloud, including in encrypted environments.
Develop training and outreach on interdiction and prevention for parents, teachers, and citizens, that emphasizes the intersection of technology and risk.	Take measures to ensure hash sets used by law enforcement are as uniform and consistent as possible, to provide feedback to tech companies about imagery in their hash sets, and to develop a uniform approach for hashes of videos.

Develop technical tools for law enforcement to conduct investigations more efficiently.	Promote public transparency across the tech sector and by relevant NGOs concerning the adoption and efficacy of child protection measures, in a manner that makes it easy to evaluate and compare.

Training

The need for training to build law enforcement capacity to address online child sexual exploitation is never ending, both because technology continues to evolve and because of turnover among personnel who investigate these crimes. This has never been truer, as the volume of digital evidence continues to grow, whether stored on numerous different types of digital devices in a home (smartphone, tablet, computer) or in the cloud. Law enforcement also needs the skillset to pursue an investigation even when some or most evidence is protected by encryption, and to execute an investigation to maximize the opportunity to access evidence in an unencrypted state. To achieve these goals, the Department will develop and deploy cutting-edge training that will be delivered on a regular basis.

Separately, extensive outreach is needed to educate the public on the risks and rewards of technology as it intersects with online child safety. The goal is not to frighten, but to empower parents, teachers, and citizens to make informed choices and to demand better and easier to use tools to protect children online, particularly in online spaces where adults and children can interact.

Partnerships

As is recognized in the Voluntary Principles, "keeping children safe from online sexual exploitation and abuse and limiting their re-victimization by preventing the sharing and viewing of CSAM can only be achieved through systematic cross-sector collaboration. Only by strengthening collaboration among governments, industry and others and drawing on our collective skills and resources will we achieve the safe online environment that our children and the global community expect and deserve."[41] In furtherance of that goal, the Department will continue to encourage companies to adopt the Voluntary Principles and to transparently describe the measures being taken within those companies to implement the Principles. This will help ensure that the endorsement of the Principles is not a meaningless gesture, and also will give the public the means to assess industry response.

Beyond the Voluntary Principles, the Global Strategic Response set forth by WeProtect Global Alliance similarly calls on the tech industry to:

- Regularly publish transparency reports on detection and prevention of CSEA online with meaningful metrics, and ensure data is supported by explainable methodology and reviewed regularly.

[41] https://www.justice.gov/opa/press-release/file/1256061/download

- [Conduct] honest appraisal of responses and prevention techniques to inform future work and efforts.

- [Provide] transparency around the innovation of tools and techniques, research, allocation of resources, and collaboration with other key stakeholders, staffing and training.[42]

The Department will endeavor to obtain, gather, and publicize such information.

To the extent that third-party NGOs, such as NCMEC, have information that illuminates whether, how, and how effectively companies are protecting children, the Department will encourage public dissemination of that information, to include seeking legislation if necessary. For example, the information shared by NCMEC about the volume of CyberTip reports sent by each company vividly illuminates the wildly varying response by industry and the impact of encryption on voluntary efforts by industry to detect CSAM on their platforms. It is critically important that such troves of information be shared with the public and policymakers.

Partnerships are also needed to harmonize several different image repositories that have been developed in the United States and are used in support of investigations in a variety of ways, the most important being to identify, locate, and rescue the children depicted in the imagery. As discussed above, while some image comparison and sharing does occur between the FBI and HSI, those image repositories are often not compared or shared with the CVIP repository, which also includes state and local submissions as well as distributed international images and videos. Neither the FBI nor HSI have access to the CVIP repository, so neither law enforcement nor NCMEC have the most up-to-date information as to which children have been identified and rescued, and which should be a priority to be identified and rescued. The Department will work with all relevant partners to address this issue, to include preparing memoranda of understanding, executive orders, or legislation as needed.

Funding and Research

Investment in two areas could yield substantial improvements in our ability to investigate online child sexual exploitation offenses. The first would be encouraging the development of new tools to facilitate gathering and analyzing digital evidence. Law enforcement is always in the position of reacting to new technological developments, so it is critical that our investigatory tools are as up to date as possible. Second, the deployment of a universal standard for hashes of videos, comparable to PhotoDNA for images, would dramatically expand the ability of both law enforcement and the tech sector to look for CSAM in video format. The explosion in CyberTips in recent years demonstrates the power of scanning for known CSAM, and yet those numbers do not include all possible versions of known videos. This gap in our collective response must be closed.

[42] https://www.weprotect.org/frameworks/gsr/