Stanford | Internet Observatory
Cyber Policy Center

The Strengths and Weaknesses of the Online Child Safety Ecosystem

Perspectives from Platforms, NCMEC, and Law Enforcement on the CyberTipline and How to Improve It

Shelby Grossman, Riana Pfefferkorn, David Thiel, Sara Shah, Alex Stamos,
Renée DiResta, John Perrino, Elena Cryst, and Jeffrey Hancock
Stanford Internet Observatory

April 22, 2024

io.stanford.edu

Contents

1 Introduction

Online child sexual exploitation is one of the most widespread and impactful abuses of the internet to cause harm.

The CyberTipline is the centralized system in the U.S. for reporting online child exploitation. It is operated by the National Center for Missing and Exploited Children (NCMEC), a nonprofit organization. If online platforms in the U.S. become aware of child sexual abuse material (CSAM)[1] federal law requires that they report it to the CyberTipline.[2] NCMEC attempts to identify the location of the user who sent and received the image, video, or in some cases text, and may attempt to locate the victim as well, then sends the report to the relevant law enforcement agencies in the U.S. and abroad.

Many trust and safety employees at online platforms, staff at civil society groups, and law enforcement officers believe that the CyberTipline process—from report submission to potential prosecution—is not living up to its potential. Those who feel this way span the ideological spectrum from civil rights activists to pro-law enforcement lobbyists. Across the board there is a sense that CyberTipline reports can be enormously valuable, but that reports that could lead to the rescue of a child being abused are not being sufficiently investigated.

In this report we show that a core issue is that two CyberTipline reports can look nearly identical to a law enforcement officer. Investigating both, however, could yield very different results: one may reveal no further illicit activity, while the other could uncover evidence of hands-on abuse. Through interviews with 66 individuals, including law enforcement officers, NCMEC staff, online platform staff, prosecutors, and defense attorneys, we identify the factors contributing to this issue, including incomplete reports from platforms, challenges NCMEC faces in rapidly improving the CyberTipline technical infrastructure, and legal constraints on NCMEC and U.S. law enforcement. We conclude with recommendations for stakeholders.

In 2023 the CyberTipline received 36,210,368 reports.[3] While 35,944,826 of these

[1] In this report we use the term child sexual abuse material, or CSAM, because it is the recommended language provided in the Luxembourg Guidelines. This is also commonly referred to as child pornography. We do not use the term "pornography" as it implies consent, which is not possible in cases involving minors. See: Interagency Working Group, "Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse," 2016, https://ecpat.org/luxembourg-guidelines/

[2] 18 U.S.C. § 2258A, https://www.law.cornell.edu/uscode/text/18/2258A.

[3] NCMEC, "U.S. Department of Justice CY 2023 Report to the Committees on Appropriations National Center for Missing and Exploited Children (NCMEC) Transparency," 2024, https://perma.cc/45XK-DYZD.

reports were from online platforms,[4] members of the public submit reports as well. Many who work to protect children online are exasperated with the use of this statistic—particularly when some inaccurately imply that 36 million reports equals 36 million victims. There are important aspects of this number to highlight. First, hundreds of reports may involve the same offender.[5] Second, NCMEC states that only 49% of all 2022 reports were actionable, either because a platform failed to provide "sufficient information for law enforcement," or because the image in the tip "is considered viral and has been reported many times"—two important but distinct phenomena.[6] Sharing CSAM is illegal in the U.S. regardless of the intent behind the share, but many images are shared in outrage or as memes without an intent to harm a child. Third, NCMEC does not specify the number of reports that are of individuals sharing old content where the child is known to authorities and is now safe. While such behavior re-traumatizes victims, and many would argue that these reports should be fully investigated as viewing CSAM is associated with hands-on abuse of children, the report itself does not provide actionable evidence to rescue a child.

Despite the spectrum of actionability among the reports, the number of reports itself nonetheless understates the amount of content platforms have identified, as a tip can contain multiple images or videos: the 36 million reports in 2023 included 105,653,162 files.[7] Although the fraction of that number represented by unique new images is not available, generally respondents told us that online-facilitated child sexual exploitation is more common than people realize.

Estimates of how many CyberTipline reports lead to arrests in the U.S. range from 5%[8] to 7.6%.[9] There are empirical and normative questions related to this number. Empirically, it is unknown what percent of reports, if fully investigated, would lead to the discovery of a person conducting hands-on abuse of a child. On the one hand, as an employee of a U.S. federal department said, "Not all tips need to lead to prosecution [...] it's like a 911 system."[10] On the other hand, there is a sense from our respondents—who hold a wide array of beliefs about law enforcement—that this number should be higher. There is a perception that more than 5% of reports, if fully investigated, would lead to the discovery of hands-on abuse.

There are additional normative questions about what should happen to people who intentionally view CSAM for their own gratification but do not engage in or

[4] NCMEC, "2023 CyberTipline Reports by Electronic Service Providers (ESP)," 2024, https://perma.cc/2DMB-V5T7.

[5] The AviaTor Project, "Save Time, Save Lives," 2021, https://perma.cc/QH7Y-ET78.

[6] NCMEC, "CyberTipline 2022 Report," 2023, https://perma.cc/V7FG-9QDM.

[7] NCMEC, "U.S. Department of Justice CY 2023 Report to the Committees on Appropriations National Center for Missing and Exploited Children (NCMEC) Transparency."

[8] *Children are Not for Sale: Examining the Threat of Exploitation of Children in the U.S. and Abroad: Hearing before The House Judiciary Subcommittee on Crime and Federal Government Surveillance*, 118th Cong. (Sept. 13, 2023) (testimony of John Pizzuro), https://perma.cc/6DQZ-XBZM.

[9] Interview with a law enforcement officer on December 4, 2023. This number is based on CyberTipline reports in 2023. Both of these statistics are based on reports sent to Internet Crimes Against Children Task Forces, which are discussed later in this section. We do not have estimates for the percent of reports that lead to arrests for reports forwarded to federal law enforcement agencies.

[10] Interview on November 17, 2023.

solicit abuse. Even if society decided that it was desirable to prosecute all of those offenders, the American judicial system lacks such capacity: "It takes milliseconds [for a platform] to detect, report, and suspend, and it takes months [...] to do an investigation," an NGO employee noted.[11] Similarly, a law enforcement officer said, "We aren't going to arrest our way out of the problem."[12]

While our research focuses on CyberTipline obstacles that make it hard to identify the worst offenders and rescue victims, we want to note that many respondents highlighted that the entire CyberTipline process is extremely valuable. One Internet Crimes Against Children Task Force (ICAC) officer—there are 61 such Task Forces throughout the U.S. and they are a primary recipient of CyberTipline reports—estimates that, for 2022, 3.8% of CyberTipline reports in his state led to a child being rescued or outreach provided to a child who was being sextorted.[13] One law enforcement officer said: "Overall NCMEC is a tremendous resource, the CyberTipline is a great tool, and NCMEC does a phenomenal job."[14] An NGO employee noted that NCMEC has more capacity than any other entity to process victim identification and they do more labeling of known and new content than any other entity.[15] Respondents felt that the fact that U.S. platforms are required to report CSAM is a strength of the system.[16] Many platforms that prioritize anonymity submit reports, as do many platforms that are not based in the U.S. and are not legally required to report.

Additionally, over time there has been more appreciation of the crime of viewing CSAM. The narrative used to be, "well he's only looking at this in the basement, is that really that bad?"[17] There is now widespread awareness in the U.S. of what a CyberTipline report is and why it's important; a NCMEC employee told us they no longer need to cold call an officer prior to sending a CyberTipline report to explain what it is.[18] Many respondents feel that the system shouldn't be disparaged simply because of the large gap between the number of reports and prosecutions. "The system is worth nurturing, preserving, and securing," a federal department employee said.[19]

Almost as soon as we began conducting interviews, we sensed conversation fatigue. People working in the online-facilitated crimes against children space are constantly discussing the system's shortcomings. "All parties are asking for feedback and feedback is not being taken into account," one platform employee told us.[20] This surprised us, as there is little public information about the system's gaps. We began starting each interview by acknowledging this conversation fatigue, and would watch as respondents vigorously nodded. One law enforcement officer said he was jaded about talking about the CyberTipline: "Nothing ever

[11] Interview on November 6, 2023.
[12] Interview with a law enforcement officer on August 18, 2023.
[13] Interview on December 4, 2023.
[14] Interview with a law enforcement officer on December 15, 2023.
[15] Interview on November 6, 2023.
[16] Interview with an NGO employee on November 6, 2023; Interview with a law enforcement officer on December 15, 2023.
[17] Interview with a platform employee on October 20, 2023.
[18] Interview on November 2, 2023.
[19] Interview on November 17, 2023.
[20] Interview on August 15, 2023.

changes."[21] We asked one investigator about hurdles with the CyberTipline process and she asked us to hold on for a minute while she pulled up her PowerPoint deck on this exact topic.[22] One law enforcement officer said: "This conversation with you is the same conversation I have had in 2015, 2016, 2017."[23]

Our sense is that these conversations are occurring behind closed doors, and we hope that by making these concerns public we will generate more informed discussions among the public and policymakers. For example, we are aware of a report on the CyberTipline commissioned by the Science & Technology Directorate in the Department of Homeland Security in 2021 and written by RTI International.[24] For unclear reasons, this report was not made public. We have read this report, and found it to be informative and fair. While the report primarily interviewed law enforcement officers, and we interviewed a broader array of stakeholders, many of the RTI International report findings resonate with the findings we present here. We hope documents like this can be made public going forward.

Key findings

The CyberTipline is enormously valuable as the key coordinating mechanism between private and public actors working in online child safety. CyberTipline reports lead to the rescue of children and prosecution of offenders. Separate from platforms' reporting obligations, their obligation to remove content is also important, as it reduces the overall amount of CSAM online, which mitigates the harms to those depicted and reduces innocent users' exposure to such material.

Law enforcement officers are overwhelmed by the high volume of CyberTipline reports they receive. However, we find that the core issue extends beyond volume: officers struggle to triage and prioritize these reports to identify offenders and reach children who are in harm. An officer might examine two CyberTipline reports – each documenting an individual uploading a single piece of CSAM – yet, upon investigation, one report might lead nowhere, while the other could uncover ongoing child abuse by the uploader. Nothing in the reports would have indicated which should be prioritized. We find that the following factors make it difficult for officers to accurately triage reports:

- Many online platforms are **not completing all of the important parts of a CyberTipline report**, or are including inaccurate data. This makes it difficult for law enforcement to identify offenders and victims.
- Relatedly, law enforcement officers are **spending valuable time processing reports that contain memes**. The use of image memes that can technically be considered illegal CSAM but that are spread without malicious intent has

[21] Interview on August 25, 2023.

[22] Interview with an investigator on August 30, 2023.

[23] Interview on September 6, 2023.

[24] "Supporting Law Enforcement Investigations to Combat Internet Crimes against Children" (RTI International, May 2021).

become, unfortunately, widespread around the world. Platforms that submit memes often fail to check the "Suspected Meme" box in their CyberTipline report.

- **NCMEC has faced challenges in rapidly implementing technological improvements** that would aid law enforcement in triage. NCMEC faces resource constraints that impact salaries, leading to difficulties in retaining personnel who are often poached by industry trust and safety teams.
- There appear to be opportunities to enrich CyberTipline reports with external data that could help law enforcement more accurately triage tips, but **NCMEC lacks sufficient technical staff to implement these infrastructure improvements** in a timely manner. Data privacy concerns also affect the speed of this work.
- For CyberTipline reports where the platform has not confirmed a human review of the image or video, or public availability of the image or video, **high-profile court decisions have caused NCMEC to stop vetting files attached to CyberTipline reports** before sending them to law enforcement, and have led many law enforcement officials to take the position that obtaining a search warrant is necessary to preserve the integrity of a potential case before viewing media linked to a report. This requirement generally delays the process of examining files to identify the most severe cases, even when the warrant acquisition process is relatively straightforward.
- Even after obtaining a warrant for the file attached to a tip, the tip on its own may **lack sufficient information for prioritization**. Multiple warrants and/or subpoenas may be needed to assess the identity of the potential offender.
- Even after knowing the identity of the potential offender, a report is just a tip. Without additional information, which at the moment is time consuming to get, **many reports look the same** and it can be difficult to know which, if investigated, is more likely to lead to the discovery of hands-on abuse.
- Constitutional concerns keep NCMEC and law enforcement from giving platforms best practices for submitting CyberTipline reports in a straightforward manner, so they **will not directly tell platforms at scale how to improve their reports** to be more actionable and easier to prioritize.
- The challenges facing the CyberTipline will be massively multiplied by the coming wave of unique, **AI-generated CSAM** that platforms will be reporting over the next several years.
- These issues would be best addressed by a concerted effort to **massively uplift NCMEC's technical and analytical capabilities**, which will require the cooperation of platforms, NCMEC, law enforcement and, importantly, the US Congress.

2 NCMEC, the CyberTipline, and ICAC Task Forces

Following grassroots advocacy, Congress authorized what is now called the National Center for Missing and Exploited Children (NCMEC) in 1984 through the Missing Children's Assistance Act of 1983.[25] This act established "a national resource center and clearinghouse to provide technical assistance to state and local governments, law enforcement agencies, and individuals in locating and recovering missing children. The purposes of this center are to coordinate public and private searches for children [...]."[26] In 2022 NCMEC received roughly 68% of its $58M in annual revenue from government contracts and grants.[27] NCMEC's government funding is primarily through the Department of Justice's Office of Juvenile Justice and Delinquency Prevention (OJJDP), and its budget is periodically reauthorized by Congress.[28] This funding supports not only the operation of the CyberTipline but also over a dozen other programs.[29]

The CyberTipline, which NCMEC created in 1998, is a tool for members of the public and electronic service providers (ESPs) to report online child sexual exploitation.[30] Staff at the CyberTipline review these reports, identify the location of the potential victim and offender from a report, and ensure the report is sent to the appropriate law enforcement agency. Reports that NCMEC geolocates to the U.S. may be sent to one of 61 regional Internet Crimes Against Children (ICAC) Task Forces—coordinating bodies that support local law enforcement with investigating cyber crimes against minors–or a federal law enforcement agency. Reports that cannot be geolocated to a specific area are made available to federal law enforcement in the U.S. In 2023, ICAC Task Forces received 908,762 reports, of which 670,491 were identified as actionable by NCMEC, and federal law enforcement received 2,106,300 reports. A small number of reports may have

[25] *Protecting Our Children Online: Hearing before The Senate Committee on the Judiciary*, 118th Cong. (Feb. 14, 2023) (testimony of Michelle DeLaune), https://perma.cc/49PH-6WG6.

[26] U.S. Senate Judiciary Committee, *Missing Children's Assistance Act of 1983: Report of the U.S. Senate Judiciary Committee on S. 2014*, 1984, https://perma.cc/T8JG-HSPA.

[27] NCMEC, "2022 Annual Report," 2022, https://perma.cc/TN7Y-F99D; ProPublica, *Full text of "Full Filing" for fiscal year ending Dec. 2022*, 2023, https://projects.propublica.org/nonprofits/organizations/521328557/202331639349301103/full.

[28] ProPublica, "Nonprofit Explorer: National Center for Missing and Exploited Children," 2023, https://perma.cc/68WP-DF2E; U.S. Senate Judiciary Committee, "Durbin, Graham Applaud Senate Passage of Legislation to Reauthorize Missing Children's Assistance Act," July 28, 2023, https://perma.cc/3VWG-552R.

[29] We note that some of these programs intersect with the CyberTipline, for example the Child Victim Identification Program and hash-sharing initiatives, but these are not the focus of this report.

[30] *Protecting Our Children Online*, *supra* note 25.

been sent to both. The 1,978 reports that lacked an internet nexus were sent to local police.[31]

The ICAC Task Force Program, also created in 1998, exists to help "local law enforcement agencies develop an effective response to technology-facilitated child sexual exploitation and Internet crimes against children."[32] This work includes training local law enforcement; in 2023 these Task Forces trained 71,000 individuals, including law enforcement officers and prosecutors.[33] Task Force funding is also administered by the OJJDP. Task Forces receive CyberTipline reports[34] and conduct an initial review. They either investigate the report in-house, send the report out to a local affiliate for investigation, or decide the report should not be investigated. Each of the Task Forces have their own policies about report prioritization. NCMEC encourages law enforcement to provide information about the outcomes of CyberTipline reports, though officers are not required by law to do so.

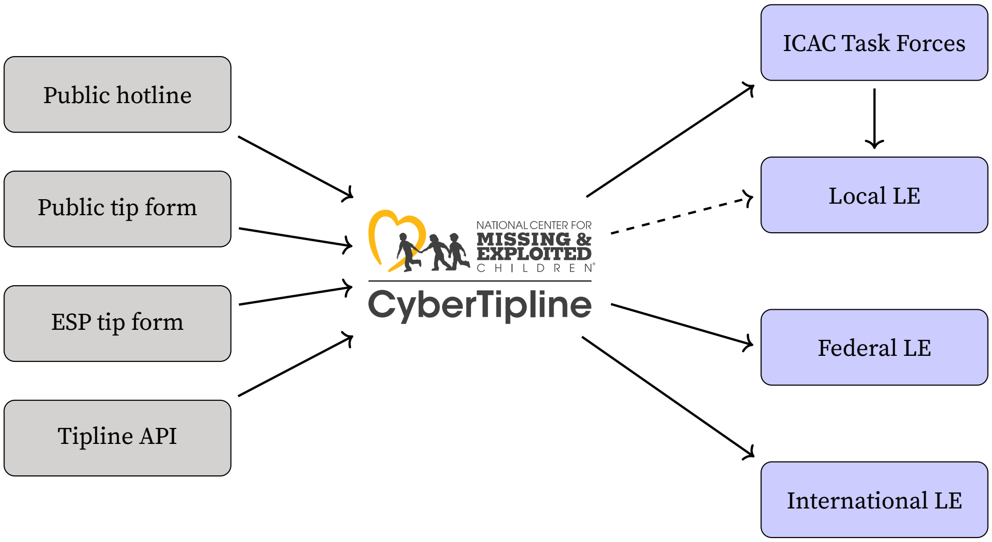


Figure 2.1: A simplified representation of the NCMEC CyberTipline routing process. Most reports come from online platforms via an API, but NCMEC also accepts reports that platforms submit manually, along with reports from members of the public. NCMEC then sends U.S. reports to federal law enforcement or ICAC Task Forces. The Task Forces may then send reports to local law enforcement. NCMEC sends a limited number of reports directly to local law enforcement agencies in the U.S. These reports typically lack an internet nexus; for example, they might include a report from a member of the public about molestation.

[31] NCMEC, "U.S. Department of Justice CY 2023 Report to the Committees on Appropriations National Center for Missing and Exploited Children (NCMEC) Transparency."

[32] Office of Juvenile Justice and Deliquency Prevention, Department of Justice, "Internet Crimes Against Children Task Force Program," 2024, https://perma.cc/E3NA-8UAE.

[33] Ibid.

[34] We use the words "report" and "tip" interchangeably.

2.1 Funding for NCMEC and the ICAC Task Forces

The Department of Justice requests, and Congress allocates, a set amount of funds for missing and exploited children work.[35] The OJJDP then distributes that funding, with a majority going to NCMEC and the ICAC Task Forces, and smaller amounts going to other entities.[36]

NCMEC receives roughly the same amount of Congressional funding for its 15 programs of work as the 61 Task Forces combined: in the 2023 fiscal year NCMEC received $41.4 million[37] and the Task Forces received $40.8 million.[38] The funding has grown over time,[39] but many believe it has not increased sufficiently. There is a perception that if NCMEC were to get a larger share of these funds, the Task Forces would receive less, and vice versa. Some respondents have suggested this creates a zero sum mentality and creates unnecessary competition between the two entities.[40]

NCMEC also receives funding from corporations and private individuals. In 2022 Meta and Old Navy were the top corporate donors; each contributed over $1 million.[41]

2.2 Insights from NCMEC's CyberTipline transparency

Over time NCMEC has provided more transparency about CyberTipline reports.[42] From this transparency we have learned that reports are increasingly about victims and offenders abroad. In 2008, 54% of tips related to victims or offenders in the United States. By 2018, 68% of tips related to Asia.[43] Of the 36 million CyberTipline reports that NCMEC received in 2023, between 91.7% and 92.5%

[35] "General Administration: Federal Funds," Department of Justice, March 2023, https://perma.cc/D2J8-LFAJ.

[36] OJJDP also distributes additional federal funding to NCMEC and the Task Forces. In the 2023 fiscal year, for example, OJJDP distributed $6 million to NCMEC from the U.S. Secret Service. See "OJJDP: National Center for Missing & Exploited Children," Office of Juvenile Justice and Delinquency Prevention, 2023, https://perma.cc/Z9SC-DYJ3; "Justice Department Awards Nearly $105 Million to Protect Children from Exploitation, Trauma and Abuse," Department of Justice, November 1, 2022, https://perma.cc/UJ6U-QUWE.

[37] "OJJDP: National Center for Missing & Exploited Children."

[38] "OJJDP: Internet Crimes Against Children Task Force Program," Office of Juvenile Justice and Delinquency Prevention, 2023, https://perma.cc/7HW2-HQ3S.

[39] "OJJDP: National Center for Missing & Exploited Children"; "OJJDP: Internet Crimes Against Children Task Force Program."

[40] Interview on January 25, 2024.

[41] NCMEC, "2022 Annual Report."

[42] This increased transparency appears to be at least partly attributed to requests from Congress. See: NCMEC, "U.S. Department of Justice CY 2023 Report to the Committees on Appropriations National Center for Missing and Exploited Children (NCMEC) Transparency"

[43] Elie Bursztein et al., "Rethinking the detection of child sexual abuse imagery on the internet," in *Proceedings of the 2019 World Wide Web Conference* (2019), 2601–7, https://doi.org/10.1145/3308558.3313482. We note that it can be difficult to interpret some of these statistics. Sometimes when NCMEC presents statistics about countries that reports were sent to the percentages add up to 100, even though there are CyberTipline reports where the victim and offender are in different countries, or a sender and a receiver are in different countries, meaning the report was sent to multiple countries.

related to a non-U.S. country.[44] In 2023, the five countries that received the most CyberTipline reports were India, the Philippines, Bangladesh, Indonesia, and Pakistan.[45] NCMEC works with Europol and Interpol, along with law enforcement in more than 150 countries and territories; these countries or territories either have direct access to the CyberTipline, or access to reports via a Homeland Security Investigations (HSI) attaché. Individual CyberTipline reports are sometimes made available to multiple law enforcement agencies. This can occur when the offender and victim are in different geographic locations.[46]

NCMEC also tracks trends in the type of CyberTipline reports. In recent years the overwhelming majority of reports—99.2% in 2023—were of the exchange or uploading of CSAM.[47] Between 2021 and 2023, however, there was a large increase in reports describing online enticement of children for sexual acts, in part reflecting growth in financial sextortion.[48]

NCMEC's annual CyberTipline Report includes a list of the number of tips submitted broken down by platform.[49] From this list we know that in 2023, 245 platforms submitted CyberTipline reports. The platforms that submitted the most tips were Facebook (17,838,422 tips / 50% of all platform tips), Instagram (11,430,007 tips / 32% of all platform tips), Google (1,470,958 tips / 4% of all platform tips), and WhatsApp (1,389,61 tips / 4% of all platform tips). These numbers should not necessarily be interpreted as indicating these platforms carry the most CSAM, but rather that they may devote more resources to identifying CSAM and submitting tips to the CyberTipline. Apple, for example, only submitted 267 CyberTipline reports in 2023, despite having many products that host user-generated content. 41% of the 245 platforms that submitted CyberTipline reports in 2023 submitted 20 or fewer reports.[50]

NCMEC can escalate CyberTipline reports to law enforcement if the report is "urgent" or indicates "a child was in imminent danger." In 2023 NCMEC escalated 63,892 tips.[51] Platforms can also escalate reports via an API field, and in exceptional cases they may reach out to law enforcement directly. A platform may label a report as escalated, but NCMEC may choose not to escalate.

NCMEC statistics show that the number of CyberTipline reports have increased dramatically. In 2014 there were 1,106,071 reports. In 2017, that number was

[44] NCMEC, "CyberTipline 2023 Report," 2024, https://www.missingkids.org/cybertiplinedata; NCMEC, "U.S. Department of Justice CY 2023 Report to the Committees on Appropriations National Center for Missing and Exploited Children (NCMEC) Transparency."

[45] NCMEC, "2023 CyberTipline Reports by Country," 2024, https://perma.cc/H2KC-CXN7. We emphasize that this observation does not suggest that these countries face greater issues with child sexual exploitation compared to others; their higher volume of reports could be attributed to factors such as population size and internet usage levels.

[46] NCMEC, "U.S. Department of Justice CY 2022 Report to the Committees on Appropriations National Center for Missing and Exploited Children (NCMEC) Transparency," 2022, https://perma.cc/4FPD-5RKJ.

[47] NCMEC, "CyberTipline 2023 Report."

[48] Ibid. Financial sextortion involves obtaining nude images—often via catfishing—and then threatening to send the images to friends and family unless the victim provides money.

[49] NCMEC, "2023 CyberTipline Reports by Electronic Service Providers (ESP)."

[50] Ibid.

[51] NCMEC, "CyberTipline 2023 Report."

10,214,753. By 2020 the number of tips had doubled to 21,751,085. NCMEC received 36,210,368 tips in 2023.

3 U.S. regulatory context

3.1 The legal basis for the CyberTipline

Federal law defines “child pornography” as a “visual depiction” that either (1) “involves the use of a minor engaging in sexually explicit conduct”; (2) “is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct”; or (3) “has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct” (aka a “morphed image”).[52] “Sexually explicit conduct,” in turn, covers sexual intercourse, bestiality, masturbation, sadistic or masochistic abuse, and “lascivious exhibition of the anus, genitals, or pubic area of any person.”[53] To determine whether something is a “lascivious exhibition,” U.S. courts use the so-called *Dost* test, a multi-factor consideration of (among other things) the focus of the image, the sexual suggestiveness of the setting, and whether the material is designed to elicit a sexual response from the viewer.[54]

Reports of CSAM are the primary focus of the CyberTipline. Federal law, 18 U.S.C. § 2258A, requires platforms to report “any facts or circumstances from which there is an apparent violation” of certain federal child sexual exploitation and abuse (CSEA) laws upon obtaining “actual knowledge” of them on their services. What information to report is left to the platform’s discretion.[55] Section 2258A also allows, but does not currently require, the reporting of “planned or imminent” violations of those laws. In enacting Section 2258A in 2008, Congress repealed its predecessor, which had governed platforms’ reporting obligations for the previous decade.[56] Originally, reports were to be made directly to law enforcement, but in 1999 the recipient was changed to “the Cyber Tip Line at [NCMEC], which shall forward that report” to designated law enforcement agencies.[57]

Section 2258A, like its predecessor statute, requires online platforms to report a violation of the federal laws regarding the selling or buying of children as well as the laws forbidding CSAM-related activities (possession, receipt, transmission, soliciting, advertisement, production both domestically and for importation into

[52] 18 U.S.C. § 2256(8), https://www.law.cornell.edu/uscode/text/18/2256.
[53] 18 U.S.C. § 2256(2).
[54] United States v. Dost, 636 F. Supp. 828 (S.D. Cal. 1986), https://perma.cc/F55S-KJU2.
[55] 18 U.S.C. § 2258A.
[56] Providing Resources, Officers, and Technology To Eradicate Cyber Threats to Our Children Act of 2008, Pub. L. No. 110-401, 122 Stat. 4229 (2008), https://perma.cc/7JW4-GNX6.
[57] Protection of Children from Sexual Predators Act of 1998, Pub. L. No. 105-314, 122 Stat. 2974 (1998), https://perma.cc/66CT-W2BW.

the U.S., etc.).[58] Not all CSEA violations must be reported: for example, Section 2258A does not presently require the reporting of child coercion, enticement, or transportation offenses,[59] child sex trafficking,[60] or violations of the child obscenity statute.[61]

3.2 Privacy constraints on the CyberTipline reporting system

The scope and implementation of the CyberTipline reporting regime are subject to statutory and constitutional protections for users' privacy online. A federal statute called the Stored Communications Act (SCA) generally forbids online platforms from voluntarily disclosing the contents of users' electronic communications to anybody (such as the government or another platform), but it makes an exception for CyberTipline reports to NCMEC.[62]

Additionally, two Fourth Amendment doctrines inform the detection, reporting, and investigation of suspected CSAM offenses online. One is the "government agent" doctrine, which requires a private party's search to abide by the Fourth Amendment if it is conducted at the government's behest. The other is the "private search" doctrine, under which law enforcement may repeat (but not exceed) a private party's independent initial search without first getting a warrant.[63]

The government agent doctrine explains why Section 2258A allows, but does not require, online platforms to search for CSAM. Indeed, the statute includes an express disclaimer that it does not require any affirmative searching or monitoring.[64] Many U.S. platforms nevertheless proactively monitor their services for CSAM, yielding millions of CyberTipline reports per year. Those searches' legality hinges on their voluntariness. The Fourth Amendment prohibits unreasonable searches and seizures by the government; warrantless searches are typically considered unreasonable.[65] The Fourth Amendment doesn't generally bind private parties, however the government may not sidestep the Fourth Amendment by

[58] 18 U.S.C. § 2258A(a)(2)(A) (duty to report "an apparent violation of section 2251, 2251A, 2252, 2252A, 2252B, or 2260 that involves child pornography"). 18 U.S.C. § 2252B, https://www.law.cornell.edu/uscode/text/18/2252B, which was not enacted until 2003, concerns the use of misleading internet domain names to trick a user into viewing obscene material or material harmful to minors. The legal definition of "child pornography" is found at 18 U.S.C. § 2256(8).

[59] 18 U.S.C. §§ 2422(b), https://www.law.cornell.edu/uscode/text/18/2422, 2423, https://www.law.cornell.edu/uscode/text/18/2423. Section 2422 covers coercion and enticement for purposes of the production of CSAM. *Id.* § 2427, https://www.law.cornell.edu/uscode/text/18/2427.

[60] 18 U.S.C. § 1591, https://www.law.cornell.edu/uscode/text/18/1591. A proposed bill that recently passed the Senate would add violations of sections 1591 (that involve a minor) and 2422(b) to the list of reporting obligations. Revising Existing Procedures On Reporting via Technology Act, S.474, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/senate-bill/474

[61] 18 U.S.C. § 1466A, https://www.law.cornell.edu/uscode/text/18/1466A.

[62] 18 U.S.C. § 2702(a), (b)(6), https://www.law.cornell.edu/uscode/text/18/2702.

[63] These two doctrines are explored in more detail in Jeff Kosseff, Online Service Providers and the Fight Against Child Exploitation: The Fourth Amendment Agency Dilemma, Jan. 18, 2021, https://www.lawfaremedia.org/article/online-service-providers-and-fight-against-child-exploitation-fourth-amendment-agency-dilemma.

[64] 18 U.S.C. § 2258A(f).

[65] Carpenter v. United States, 585 U.S. __, 138 S. Ct. 2206, 2221 (2018) (citations omitted), https://perma.cc/D3J4-WAQS.

making a private entity conduct a search that it could not constitutionally do itself. If a private party acts as the government's "instrument or agent" rather than "on his own initiative" in conducting a search, then the Fourth Amendment does apply to the search.[66] That's the case where a statute either mandates a private party to search or "so strongly encourages a private party to conduct a search that the search is not primarily the result of private initiative."[67] And it's also true in situations where, with the government's knowledge or acquiescence, a private actor carries out a search primarily to assist the government rather than to further its own purposes, though this is a case-by-case analysis for which the factors evaluated vary by court.[68]

Without a warrant, searches by government agents are generally unconstitutional. The usual remedy for an unconstitutional search is for a court to throw out all evidence obtained as a result of it (the so-called "exclusionary rule").[69] If a platform acts as a government agent when searching a user's account for CSAM, there is a risk that the resulting evidence could not be introduced against the user in court, making a conviction (or plea bargain) harder for the prosecution to obtain. This is why Section 2258A does not and could not require online platforms to search for CSAM: it would be unconstitutional and self-defeating.

In CSAM cases involving CyberTipline reports, defendants have tried unsuccessfully to characterize platforms as government agents whose searches were compelled by Section 2258A and/or by particular government agencies or investigators. But courts, pointing to the statute's express disclaimer language (and, often, the testimony of investigators and platform employees), have repeatedly held that platforms are not government agents and their CSAM searches were voluntary choices motivated mainly by their own business interests in keeping such repellent material off their services.[70]

3.2.1 The *Ackerman*, *Keith*, and *Wilson* cases

In a landmark case called *Ackerman*, one federal appeals court held that NCMEC is a "governmental entity or agent." Writing for the Tenth Circuit panel, then-

[66] Skinner v. Railway Lab. Execs. Ass'n, 489 U.S. 602, 614 (1989), https://perma.cc/7D79-HCLH.

[67] United States v. Stevenson, 727 F.3d 826, 829 (8th Cir. 2013) (cleaned up), https://perma.cc/2SPF-FD9K.

[68] United States v. Steiger, 318 F.3d 1039, 1045 (11th Cir. 2003), https://perma.cc/266U-CCR9; United States v. Walther, 652 F.2d 788, 792–93 (9th Cir. 1981), https://perma.cc/RE3Y-422Q. The First Circuit also considers the government's "intent and the degree of control it exercises over the search and the private party." United States v. Pervaz, 118 F.3d 1, 6 (1st Cir. 1997), https://perma.cc/P4N6-LP7W. See generally Kosseff, *supra* note 63, at 4–6 (discussing different tests for government agency developed by various courts).

[69] Christie Nicholson, "The Fourth Amendment and the 'Exclusionary Rule'," *Findlaw*, last reviewed October 13, 2023, https://www.findlaw.com/criminal/criminal-rights/the-fourth-amendment-and-the-exclusionary-rule.html.

[70] E.g., *Stevenson*, 727 F.3d at 830 (Section 2258A did not turn AOL into a state actor); United States v. Wolfenbarger, No. 22-10188, 2024 U.S. App. LEXIS 87, at *3 (9th Cir. Jan. 3, 2024) (unpub.), https://perma.cc/3PJK-ZJE9 (affirming district court's decision that Yahoo was not a government agent); United States v. Rosenow, 50 F.4th 715, 730 (9th Cir. 2022), https://perma.cc/TJM8-YGL9 (same); United States v. Ringland, 966 F.3d 731 (8th Cir. 2020), https://perma.cc/AK44-NJVB (same as to Google).

judge Neil Gorsuch concluded that NCMEC counts as a government entity in light of NCMEC's authorizing statutes and the functions Congress gave it to perform, particularly its CyberTipline functions.[71] Even if NCMEC isn't itself a governmental entity, the court continued, it acted as an agent of the government in opening and viewing the defendant's email and four attached images that the online platform had (as required) reported to NCMEC. The court ruled that those actions by NCMEC were a warrantless search that rendered the images inadmissible as evidence.[72] *Ackerman* followed a trial court-level decision, *Keith*, which had also deemed NCMEC a government agent: its review of reported images served law enforcement interests, it operated the CyberTipline for public not private interests, and the government exerts control over NCMEC including its funding and legal obligations.[73] As an appellate-level decision, *Ackerman* carries more weight than *Keith*, but both have proved influential.[74]

The private search doctrine is the other Fourth Amendment doctrine commonly raised in CSAM cases. It determines what the government or its agents may view without a warrant upon receiving a CyberTipline report from a platform. As said, the Fourth Amendment generally does not apply to searches by private parties. "If a private party conducted an initial search independent of any agency relationship with the government," the private search doctrine allows law enforcement (or NCMEC) to repeat the same search so long as they do not exceed the original private search's scope.[75] Thus, if a platform reports CSAM that its searches had flagged, NCMEC and law enforcement may open and view the files without a warrant so long as someone at the platform had done so already.[76] The CyberTipline form lets the reporting platform indicate which attached files it has reviewed, if any,[77] and which files were publicly available.

For files that were not opened by the platform (such as where a CyberTipline submission is automated without any human review), *Ackerman* and a 2021 Ninth Circuit case called *Wilson* hold that the private search exception does not apply, meaning the government or its agents (i.e., NCMEC) may not open the unopened files without a warrant.[78] *Wilson* disagreed with the position, adopted by two other appeals-court decisions, that investigators' warrantless opening of unopened files

[71] United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016), https://perma.cc/RE62-RJ7A.

[72] *Id.* at 1300–08.

[73] United States v. Keith, 980 F. Supp. 2d 33 (D. Mass. 2013), https://perma.cc/99BG-5CJ3. The platform (which the court ruled was not a government agent) had not opened the email attachments it sent to NCMEC, which did review them before reporting them to law enforcement. *Id.* at 37–38, 40.

[74] Another case split the baby as to NCMEC's proper characterization: while "not convinced that NCMEC is a governmental entity," the court went along with "viewing NCMEC as an agent of law enforcement." United States v. Coyne, 387 F. Supp. 3d 387 (D. Vt. 2018), https://perma.cc/U4KE-45KC (collecting cases finding NCMEC to be a government entity or agent under the Fourth Amendment).

[75] *Ringland*, 966 F.3d at 736; see also United States v. Jacobsen, 466, U.S. 109 (1984), https://perma.cc/2QA7-BN5T.

[76] *Ringland*, 966 F.3d at 737.

[77] *Id.* at 733. If the platform fails to check the "reviewed" box for a specific file, that does not necessarily mean no human reviewed the file (as we discuss later on), merely that more information besides the CyberTipline report would be needed to confirm whether it had been reviewed or not.

[78] *Ackerman*, 831 F.3d at 1305–7; United States v. Wilson, 13 F.4th 961, 971–74 (9th Cir. 2021), https://perma.cc/CND9-NMPN. The remedy for the improper warrantless search is exclusion. *Wilson*, 13 F.4th at 964; *Ackerman*, 831 F.3d at 1308.

is permissible if the files are hash matches for files that had previously been viewed and confirmed as CSAM by platform personnel.[79] *Ackerman* concluded by predicting that law enforcement "will struggle not at all to obtain warrants to open emails when the facts in hand suggest, as they surely did here, that a crime against a child has taken place."[80]

To sum up: Online platforms' compliance with their CyberTipline reporting obligations does not convert them into government agents so long as they act voluntarily in searching their platforms for CSAM. That voluntariness is crucial to maintaining the legal viability of the millions of reports platforms make to the CyberTipline each year. This imperative shapes the interactions between platforms and U.S.-based legislatures, law enforcement, and NCMEC. Government authorities must avoid crossing the line into telling or impermissibly pressuring platforms to search for CSAM or what to search for and report. Similarly, platforms have an incentive to maintain their CSAM searches' independence from government influence and to justify those searches on rationales "separate from assisting law enforcement."[81] When platforms (voluntarily) report suspected CSAM to the CyberTipline, *Ackerman* and *Wilson* interpret the private search doctrine to let law enforcement and NCMEC warrantlessly open and view only user files that had first been opened by platform personnel before submitting the tip or were publicly available.

Ackerman, *Keith*, and *Wilson* may seem like isolated decisions, but they have profoundly affected the CyberTipline ecosystem. As this paper will discuss, there are many shortcomings in the current CyberTipline regime, including the type, volume, quality, availability, reliability, consistency, formatting, and overall usefulness of the information law enforcement authorities receive from CyberTipline reports. But constitutional considerations make it a fraught process for the government, NCMEC, and platforms to communicate with one another about desired improvements.

The current CyberTipline reporting system would effectively collapse if platforms' searches were deemed to be state action rather than voluntary private conduct: proactive CSAM monitoring by U.S. platforms would have to stop. That is unimaginable now that it is responsible for tens of millions of CyberTipline reports annually.[82] Preserving the viability of that practice has emerged as a common goal of stakeholders in the child safety ecosystem: platforms, NCMEC, law enforcement, and other government actors. When European privacy law imperiled voluntary CSAM scanning in the EU, the law changed.[83] When Fourth Amendment

[79] United States v. Miller, 982 F.3d 412, 428–31 (6th Cir. 2020), https://perma.cc/Q2D3-EBR9; United States v. Reddick, 900 F.3d 636, 637–39 (5th Cir. 2018), https://perma.cc/BXC8-W2L7. But see *Keith*, 980 F. Supp. 2d at 43 (rejecting equivalency between hash matching and a human viewing the contents of a file).

[80] *Ackerman*, 831 F.3d at 1309.

[81] Kosseff, *supra* note 63, at 8.

[82] NCMEC, "2023 CyberTipline Reports by Electronic Service Providers (ESP)."

[83] Julia Tar, "Commission highlights data shortfall in interim child sexual abuse regulation," *Euractiv*, December 19, 2023, https://www.euractiv.com/section/law-enforcement/news/commission-highlights-data-shortfall-in-interim-child-sexual-abuse-regulation/.

cases threatened the admissibility in U.S. courts of material platforms reported to the CyberTipline, stakeholders' practices changed.

Legal timeline of the CyberTipline

1984	NCMEC established
1998	CyberTipline created
1998	Protection of Children from Sexual Predators Act (requiring platforms to report CSAM to law enforcement agencies)
1999	Statutory recipient of platform reports changed from law enforcement to CyberTipline
2008	PROTECT Our Children Act (modifying platforms' reporting requirements, authorizing additional optional reporting)
2013	*U.S. v. Keith* ruling (NCMEC is a government agent)
2016	*U.S. v. Ackerman* ruling (NCMEC is a government entity or agent)
2021	*U.S. v. Wilson* ruling (government cannot open unopened files without warrant)

4 Methods

Our findings are based primarily on semi-structured interviews. We used a variety of methods to recruit respondents. For platforms we emailed the law enforcement outreach contacts that platforms listed on a website for law enforcement. To recruit law enforcement, we reached out to people who attended a relevant law enforcement conference[84] and had shared their email address on the conference app. We also hand delivered letters to local police departments, and reached out to ICAC Task Forces using a website that provides a tool to message them. To recruit civil society respondents we emailed the general email address on the websites of relevant groups. For most categories of respondents we also leveraged our existing contacts.

We additionally visited NCMEC's headquarters in Alexandria, Virginia for three days in January and February 2024. During this visit NCMEC staff provided what we believe to be an unprecedented level of transparency. They spent hours with us answering over two dozen questions we had emailed in advance. We had a meeting with their technical team, who walked us through their data infrastructure and development roadmap. And they had an analyst process CyberTipline reports in front of us in real time (the analyst viewed files prior to sharing their screen). Throughout these and other sessions, NCMEC staff answered all of our questions, and did not cut us off when sessions went far over time. We conducted three additional Zoom interviews with NCMEC staff. NCMEC staff told us that this was the first time they had provided this level of transparency to an academic group.

In total, we interviewed 66 people. We estimate that the response rate was approximately 25%. We interviewed 12 people from civil society (both in the U.S. and abroad), 15 current and former online platform employees, eight NCMEC employees, seven federal civil servants, four defense attorneys, three employees of companies that help law enforcement outside of the U.S. enrich and triage CyberTipline reports, two prosecutors, one attorney who works with victims, and one lobbyist. We spoke with eight individuals who have worked or are currently working in U.S. law enforcement: five people at ICAC Task Forces and three local law enforcement officers who work for departments that are Task Force-affiliates.[85] We also spoke with five members of non-U.S. law enforcement.

All but one of the U.S. law enforcement officers who agreed to speak with us specialize in crimes against children. This may not seriously affect the representativeness of our sample as local law enforcement rarely receive CyberTipline reports unless their department is affiliated with a Task Force. Still, our findings

[84] The Crimes Against Children Conference in August 2023. https://cacconference.org

[85] To fully anonymize these respondents, we refer to all of them as "law enforcement officers."

may be biased toward the perspective of law enforcement with more experience investigating these reports. This suggests that we may be understating the challenges in investigating CyberTipline reports.

If we heard a critique of an actor in an interview—for example a law enforcement officer unhappy with platform behavior—we took that critique to a platform to hear their perspective. In part for this reason we interviewed many respondents twice or three times.

With their consent, we granted NCMEC respondents personal but not institutional anonymity, as we did not think it was feasible to provide their perspective without making clear where it came from. We provided all other respondents with both personal and institutional anonymity. Our research received approval from Stanford University's Institutional Review Board[86] under protocol #70974.

[86] https://researchcompliance.stanford.edu

5 Findings: Platforms

Key findings

- Initiating CSAM detection is time consuming.
- Beginning CSAM reporting is often confusing, may require personal networking, and integration with the reporting API can be cumbersome.
- NCMEC offers onboarding calls with platforms; however, possibly due to legal constraints, no written documentation on best reporting practices is provided. With platform staff turnover, knowledge from this onboarding call can be quickly lost.
- Platforms' failure to label files as potential memes leads to considerable inefficiencies, burdening law enforcement with unproductive work.
- Ambiguity and disparate legal interpretations among platforms regarding the "File Viewed by Company" checkbox result in complications for law enforcement agencies.
- Platforms weigh the well-being of their moderators and capacity constraints when deciding if a file should be reviewed by a person before submitting a report.
- The CyberTipline reporting form lacks a dedicated and structured field for the submission of chat-related content, such as sextortion messaging.
- Challenges specific to low-volume reporters:
  - ↣ Although NCMEC maintains ongoing communication with major reporting entities, many low-volume reporters do not receive such consistent feedback.
  - ↣ Many platforms are not members of the Tech Coalition, missing out on crucial peer guidance regarding CyberTipline reporting.
  - ↣ Low-volume reporters in particular find the apparent lack of investigative follow-up on their submissions disheartening, though this is true for higher-volume reporters as well.

5.1 Establishing CSAM detection and reporting systems

Platform employees tasked with establishing a CSAM detection and reporting system will face several challenges. "At some point every company reaches the decision to commit to solving this problem," an NGO employee said. "But before they get to that stage, they aren't talking to people, they're not engaging, maybe there's bad press on them out there, or maybe they're flying under the radar. But any platform that facilitates [user-generated content] is going to have this problem regardless of medium."[87] A platform that decides to scan for and remove CSAM must establish platform policies around permitted and prohibited content, must develop technological tools for conducting this work at scale, must integrate

[87] Interview on October 18, 2023.

reporting to the CyberTipline, and must consider how to handle the well-being of employees exposed to this disturbing material in the course of their moderator work.

Trust and safety teams may begin by implementing a service like Microsoft's PhotoDNA, which identifies images similar to known CSAM using a perceptual hash.[88] Platforms can customize how they use PhotoDNA, selecting specific image hash databases for integration. PhotoDNA can hinder the speed of image uploads, prompting the need for technical enhancements to streamline its integration.[89] At first, using PhotoDNA may overwhelm a platform that is newly trying to tackle CSAM. One respondent told us about a company that started running PhotoDNA across their platform. In just 90 minutes, PhotoDNA had detected a volume of content so great (including many false positives) that it would take their small existing moderator team eight months to review.[90] Upon detecting CSAM, platforms are legally bound to report it "as soon as reasonably possible," and to "preserve the contents provided in the report for 90 days after the submission to the CyberTipline."[91] These requirements may be tough to meet if an automated detection system immediately creates months of work, illustrating the perils to (especially smaller) platforms of going in underprepared for the large and complex task of CSAM mitigation.

Platforms employ various methods to detect CSAM, including hash matching, user reports, trusted flagger programs,[92] proprietary automated detection technologies, and manual investigations by employees. Some platforms maintain their own hash dataset, which one former platform employee described as being very carefully gated. At their previous workplace, a user account would be suspended if it contained an image matching the hash database, and the offending material reported to the CyberTipline. That suspension would affect the user's access to all the company's various products. Such measures are drastic, and the platform was diligent in ensuring any action taken was justified by the presence of actual CSAM. They said an image would only be added to the internal hash dataset after a platform employee had personally verified it as apparent CSAM, emphasizing the significant effort put into preserving the integrity of the hash set.[93]

There are four methods for submitting tips to the CyberTipline: the manual reporting form available to the public,[94] the call center, the manual reporting form for ESPs, and the API. For platforms reporting more than a few tips monthly, the API is the most efficient option. However, platform employees may not know how to initiate reporting tips through NCMEC's API. At the time of this writing, it appears that the only guidance on NCMEC's website about initiating API use is located at https://www.missingkids.org/theissues/csam. This page, which

[88] See the box on the following page for a primer on hashing technology and hash databases.

[89] Interview with a platform employee on December 7, 2023.

[90] Interview with an NGO employee on November 6, 2023. An employee of a platform described a similar experience of being overwhelmed with the number of PhotoDNA hits that his company wanted to manually review, even though many were false positives (interview on December 7, 2023).

[91] 18 U.S.C. § 2258A.

[92] See, for example, https://support.google.com/youtube/answer/7554338?hl=en.

[93] Interview on September 22, 2023.

[94] https://report.cybertip.org/reporting.

is presented as a way to learn about CSAM in general, includes: "Are you an ESP who would like to register with NCMEC? Click here." This links to an email address through which platforms can inquire about starting with the API. According to our interviews, most employees charged with setting up CyberTipline integration typically start by obtaining a contact email for someone at NCMEC through their professional networks, as summed up by one respondent: "You have to know someone who knows someone" to get started.[95]

A brief beginner's guide to hashing

Platforms commonly detect CSAM through the use of image hash databases. These hashes are a unique code that maps to an image of known CSAM, allowing platforms to compare images on their platforms to known CSAM without accessing the comparison image. Various algorithms can be used to assess the match. Cryptographic algorithms such as MD5 are used for exact matches: if an image is manipulated in any way (even resizing, which may occur on image upload), this type of algorithm will not detect a match.

Perceptual hashing algorithms[a] such as PhotoDNA (PhotoDNA is also a service[b] that uses the PhotoDNA algorithm) will detect fuzzy matches—for example, a known image that was compressed or manipulated. While highly accurate, such algorithms can occasionally generate false positives, claiming there is a match when in fact the two images are unique. Microsoft's PhotoDNA service allows platforms to choose which hash databases it wants to match on: for example, platforms could choose to use a NCMEC-provided hash database, the Internet Watch Foundation hash database, and/or a Tech Coalition database (see Figure 5.1 on the next page).

Another perceptual hashing algorithm, the Meta-developed open-source PDQ,[c] allows platforms to adjust their tolerance for false positives or false negatives. There are additional algorithms for video content, such as TMK+PDQF[d] and vPDQ.[e] Platforms, particularly larger ones, may also have their own machine-learning classifiers for identifying previously unknown CSAM. The platform can hash these images for their internal detection going forward, and can also share these hashes with shared hash databases so that other platforms can detect the media.[f]

[a] Hany Farid, "An Overview of Perceptual Hashing," *Journal of Online Trust and Safety* 1, no. 1 (October 2021), https://doi.org/10.54501/jots.v1i1.24.

[b] "PhotoDNA," Microsoft, accessed February 19, 2024, https://www.microsoft.com/en-us/photodna.

[c] Facebook, "The TMK+PDQF Video-Hashing Algorithm and the PDQ Image-Hashing Algorithm," 2019, https://github.com/facebook/ThreatExchange/blob/master/hashing/hashing.pdf.

[d] Ibid.

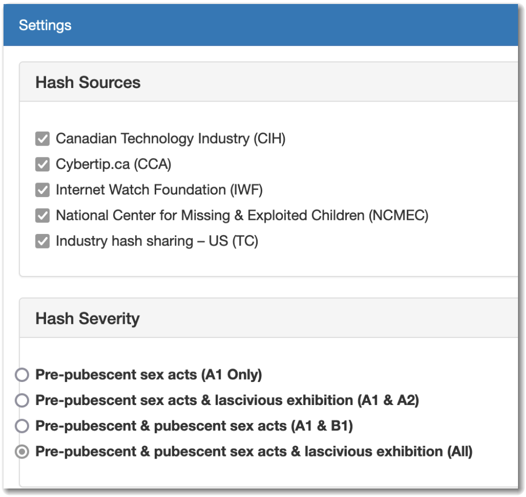
[e] Facebook, "vPDQ," 2022, https://github.com/facebook/ThreatExchange/tree/main/vpdq.

[f] Interview on September 22, 2023.

Once NCMEC provides a platform with an API key and the corresponding manual, integrating their workflow with the reporting API can still present challenges. The API is XML-based, which requires considerably more code to integrate with than simpler JSON-based APIs and may be unfamiliar to younger developers. NCMEC is aware that this is an issue.[96] "Surprisingly large companies are using the manual

[95] Interview with an NGO employee on October 18, 2023. One respondent who works at a platform reported a related issue: they struggled to get information on how to plug in to a separate NCMEC program: "I had to chase them for a very long time to get that information," they said. (Interview on November 6, 2023.)

[96] Interview with NCMEC staff between January 30 and February 1, 2024.



Settings

Hash Sources

☑ Canadian Technology Industry (CIH)
☑ Cybertip.ca (CCA)
☑ Internet Watch Foundation (IWF)
☑ National Center for Missing & Exploited Children (NCMEC)
☑ Industry hash sharing – US (TC)

Hash Severity

○ Pre-pubescent sex acts (A1 Only)
○ Pre-pubescent sex acts & lascivious exhibition (A1 & A2)
○ Pre-pubescent & pubescent sex acts (A1 & B1)
● Pre-pubescent & pubescent sex acts & lascivious exhibition (All)

Figure 5.1: Configurable settings for hash databases and severity in Microsoft's PhotoDNA cloud platform.

form," one respondent said.[97] One respondent at a small platform had a more moderate view; he thought the API was fine and the documentation "good."[98] But another respondent called the API "crap."[99]

Reporting images and videos through NCMEC's API is streamlined, but many platforms lack a structured method for reporting messaging content, such as direct message conversations that may indicate an adult grooming a child or instances of sextortion (extorting nude content). One platform employee told us that reporting direct messaging is arduous.[100] Platforms currently have two options: they can include the chat text in an "additional information" open response field or they can include it as a file upload. The former approach will increase the likelihood that the report is actionable, as the latter approach has the issue associated with all file attachments: if the "File Viewed by Company" box is not checked, NCMEC cannot view the file and law enforcement will generally not view the file without a search warrant. NCMEC does not currently have a structured format for chat content.[101]

Platforms will additionally face policy decisions. While prohibiting illegal content is a standard approach, platforms often lack specific guidelines for moderators on how to interpret nuanced legal terms such as "lascivious exhibition."[102] This term is crucial for differentiating between, for example, an innocent photo of a baby in a bathtub, and a similar photo that appears designed to show the baby in a way that would be sexually arousing to a certain type of viewer. Trust and safety employees will need to develop these policies and train moderators.

[97] Interview with an NGO employee on October 18, 2023.
[98] Interview on December 7, 2023. API documentation at "CyberTipline Reporting API Technical Documentation," NCMEC, accessed February 21, 2024, https://report.cybertip.org/ispws/documentation/.
[99] Interview with an NGO employee on November 6, 2023.
[100] Interview on November 6, 2023.
[101] Interview with NCMEC staff between January 30 and February 1, 2024.
[102] 18 U.S.C. § 2256, https://www.law.cornell.edu/uscode/text/18/2256.

There's also growing concern about the psychological impact on human content moderators who are repeatedly exposed to CSAM.[103] To protect moderators, the platform (or its contractors) must develop wellness resources. This includes behavioral measures such as access to counseling or rotational requirements, and technical measures to reduce harm, such as displaying images in black and white. Moreover, to minimize the exposure of additional staff to harmful content, platforms may need to enable moderators to remove content directly without involving an engineer or another employee in the process.

5.2 Platforms and law enforcement

Once a platform starts reporting, they may start receiving requests from law enforcement. These often include demands to extend data preservation, a procedure that is relatively easy for law enforcement but can pose challenges for a small platform if they have not yet established appropriate infrastructure. In addition to these requests, platforms may receive subpoenas for additional account information not included in the initial report. This may mean time consuming direct conversations with law enforcement. "Law enforcement hate portals, they want to talk to a person," an NGO employee with industry experience told us. "That doesn't go well when your law enforcement liaison team [is] one person."[104]

Law enforcement may also be frustrated with the quality of information in early reports: "Every company does this clumsy learning process of [figuring out] what the most helpful information is to provide."[105] For instance, one platform initially only provided login IP addresses, which are less helpful than the IP addresses used during the upload of the media in question. NCMEC does onboarding calls with platforms where they explain what information makes a report actionable, but if there is staff turnover at the platform the new point person may lack this information. NCMEC has regular meetings to provide feedback on report quality with at least some of the high-volume reporting platforms,[106] but the majority of reporting platforms do not get this level of access. This is likely due to capacity issues, as 245 platforms reported CyberTips in 2023.[107] Possibly due to legal considerations, NCMEC does not put information about what makes a report actionable for law enforcement in writing.[108] Beyond requesting a call with NCMEC, it is not clear to us if it is possible for a platform with few

[103] R. Spence et al., "The psychological impacts of content moderation on content moderators: A qualitative study," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 17, no. 4 (2023), https://doi.org/10.5817/CP2023-4-8; Casey Newton, "The Trauma Floor," *The Verge*, February 25, 2019, https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona.

[104] Interview on October 6, 2023.

[105] Interview on October 18, 2023.

[106] Interview with a former platform employee on December 20, 2023.

[107] NCMEC, "CyberTipline 2023 Report."

[108] Interviews with NCMEC staff between January 30 and February 1, 2024. NCMEC staff emphasized that they do not tell platforms what information to include in the report. Rather, they tell platforms that law enforcement will not be able to investigate the platform's report unless it has certain information, such as offender information.

connections to get information on which types of information are most valuable to law enforcement.

Employees in trust and safety roles, particularly those new to the field, might mistakenly escalate reports that don't require escalation. For instance, upon encountering a distressing image, they might not realize that the image is several decades old and the child involved has already been identified. As a result, in addition to submitting a CyberTipline report, they might reach out directly to law enforcement thinking someone's life is in immediate danger, causing frustration for both parties.[109] The Tech Coalition, an industry membership-based group to promote best practices in protecting children online, can mentor platforms on this process, but many platforms are not Tech Coalition members.[110] The lowest tier membership costs just $10,000 per year and provides all member resources, but very small platforms might still not be able to afford that, and the 41% of platforms that submitted 20 or fewer reports in 2023 may not be incentivized to pay the fee.[111] Platforms may also not meet the basic membership requirements, which include having published community standards on child sexual exploitation.[112]

5.3 Reporting considerations

Once a platform integrates with NCMEC's CyberTipline reporting API, they are incentivized to overreport. Consider an explicit image of a 22-year-old who looks like they could be 17: if a platform identified the content internally but did not file a report and it turned out to be a 17-year-old, they may have broken the law. In such cases, they will err on the side of caution and report the image. Platform incentives are to report any content that they think is violative of the law, even if it has a low probability of prosecution. This conservative approach will also lead to reports from what Meta describes as "non-malicious users"—for instance, individuals sharing CSAM in outrage.[113] Although such reports could theoretically yield new findings, such as uncovering previously unknown content, it is more likely that they overload the system with extraneous reports. The CyberTipline reports do give platforms a space and schema for categorizing content severity (see Figure 5.2 on the following page).

The CyberTipline ESP reporting form and API include several other fields platforms can mark to help prioritize reports (Figure 5.3 on the next page). One field allowing platforms to label an image as a potential meme, signaling law enforcement to deprioritize the tip. Meme content is something that is widely shared because some users find it funny or outrageous. Usage of this field varies: some platforms apply it carefully, while others may not use it at all. There is a related

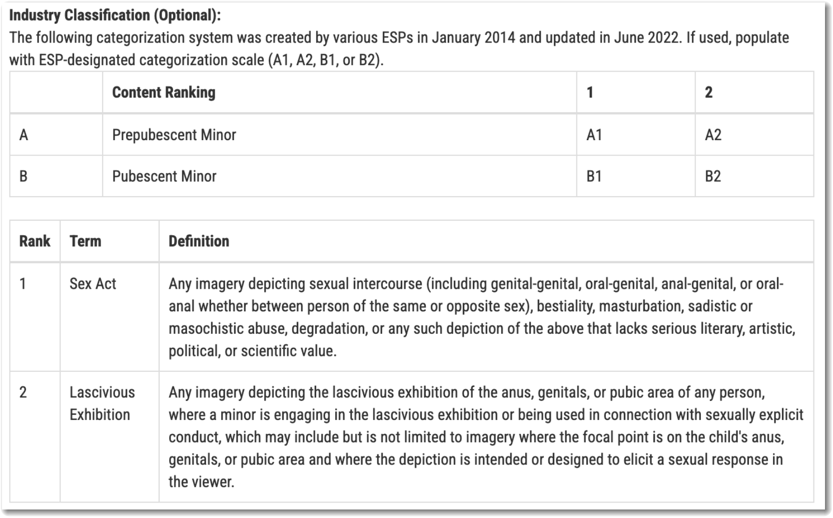
[109] This generalized account of the experience a platform might have was shared by an NGO employee with experience in industry on November 6, 2023.

[110] https://www.technologycoalition.org/.

[111] https://www.technologycoalition.org/membership/tiers.

[112] https://www.technologycoalition.org/membership/criteria.

[113] John Buckley, Malia Andrus, and Chris Williams, "Understanding the intentions of Child Sexual Abuse Material (CSAM) sharers," *Meta* (blog), February 23, 2021, https://research.facebook.com/blog/2021/2/understanding-the-intentions-of-child-sexual-abuse-material-csam-sharers/.



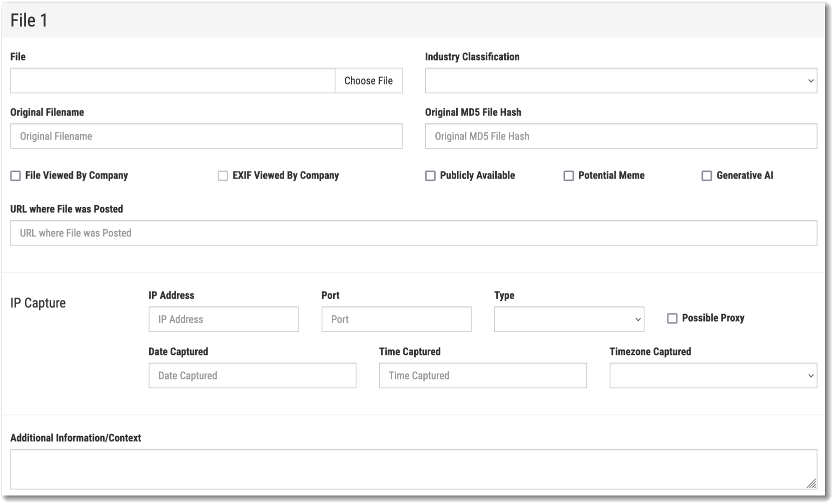
Industry Classification (Optional):
The following categorization system was created by various ESPs in January 2014 and updated in June 2022. If used, populate with ESP-designated categorization scale (A1, A2, B1, or B2).

	Content Ranking	**1**	**2**
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	**Term**	**Definition**
1	Sex Act	Any imagery depicting sexual intercourse (including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction of the above that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any imagery depicting the lascivious exhibition of the anus, genitals, or pubic area of any person, where a minor is engaging in the lascivious exhibition or being used in connection with sexually explicit conduct, which may include but is not limited to imagery where the focal point is on the child's anus, genitals, or pubic area and where the depiction is intended or designed to elicit a sexual response in the viewer.

Figure 5.2: Classification that reporting platforms can use to indicate file severity, as seen on the CyberTipline form on February 12, 2024.

type of content that NCMEC calls "viral". Both the platform and NCMEC can label content "viral", however NCMEC uses a cross-platform definition.



File 1

File
Choose File

Industry Classification

Original Filename
Original Filename

Original MD5 File Hash
Original MD5 File Hash

□ **File Viewed By Company** □ **EXIF Viewed By Company** □ **Publicly Available** □ **Potential Meme** □ **Generative AI**

URL where File was Posted
URL where File was Posted

IP Capture

IP Address
IP Address

Port
Port

Type

□ **Possible Proxy**

Date Captured
Date Captured

Time Captured
Time Captured

Timezone Captured

Additional Information/Context

Figure 5.3: An excerpt from the CyberTipline manual form for online platforms, as seen on February 12, 2024. This shows important file-level checkboxes, including "File Viewed by Company," "Potential Meme," and "Generative AI."

Memes and viral content pose a huge challenge for CyberTipline stakeholders. In the best case scenario, a platform checks the "Potential Meme" box and NCMEC automatically sends the report to an ICAC Task Force as "informational," which appears to mean that no one at the Task Force needs to look at the report.[114]

In practice, a platform may not check the "Potential Meme" box (possibly due to

[114] Multiple respondents pointed out that depending on context a particular share of a meme could be worth investigating. But given the volume of CyberTipline reports, Task Forces do not appear to be investigating memes and want them labeled "informational." (Interview with a foreign government official on February 27, 2024; Interview with a platform employee on March 6, 2024.)

fixable process issues or minor changes in the image that change the hash value)[115] and also not check the "File Viewed by Company" box. In this case NCMEC is unable to view the file, due to the *Ackerman* and *Wilson* decisions as discussed in Chapter 3. A Task Force could view the file without a search warrant and realize it is a meme, but even in that scenario it takes several minutes to close out the report. At many Task Forces there are multiple fields that have to be entered to close the report, and if Task Forces are receiving hundreds of reports of memes this becomes hugely time consuming.[116] Sometimes, however, law enforcement may not realize the report is a meme until they have invested valuable time into getting a search warrant to view the report.

NCMEC recently introduced the ability for platforms to "batch report" memes after receiving confirmation from NCMEC that that meme is not actionable. This lets NCMEC label the whole batch as informational, which reduces the burden on law enforcement.[117]

We heard about an example where a platform classified a meme as CSAM, but NCMEC (and at least one law enforcement officer we spoke to about this meme) did not classify it as CSAM. NCMEC told the platform they did not classify the meme as CSAM, but according to NCMEC the platform said because they do consider it CSAM they were going to continue to report it. Because the platform is not consistently checking the "Potential Meme" box, law enforcement are still receiving it at scale and spending substantial time closing out these reports.[118]

There is a related challenge when a platform neglects to mark content as "viral". Most viral images are shared in outrage, not with an intent to harm. However, these viral images can be very graphic. The omission of the "viral" label can lead law enforcement to mistakenly prioritize these cases, unaware that the surge in reports stems from multiple individuals sharing the same image in dismay.[119]

We spoke to one platform employee about the general challenge of a platform deeming a meme CSAM while NCMEC or law enforcement agencies disagree. They noted that everyone is doing their best to apply the *Dost* test.[120] Additionally, there is no mechanism to get an assurance that a file is not CSAM: "No one blesses you and says you've done what you need to do. It's a very unsettling place to be."[121] They added that different juries might come to different conclusions about what counts as CSAM, and if a platform fails to report a file that is later deemed CSAM the platform could be fined $300,000[122] and face significant public backlash: "The incentive is to make smart, conservative decisions."

[115] Interview with a platform employee on March 6, 2024.

[116] Interview with a law enforcement officer on February 5, 2024. The issue of time-consuming report closures was also raised in an interview with an investigator in another high-income country on February 27, 2024.

[117] Interview with NCMEC staff on January 31, 2024.

[118] Interview with NCMEC staff between January 30 and February 1, 2024; Interview with a law enforcement officer on February 5, 2024.

[119] Interview with NCMEC staff between January 30 and February 1, 2024.

[120] See Section 3.1.

[121] Interview with platform employee on March 6, 2024.

[122] 18 U.S.C. § 2258A.

An investigator abroad voiced frustration over CyberTipline reports that lack context for an image or video. For instance, if an image—perhaps a meme—is preceded by the sentence "I am going to do this to your sports team," the next steps for law enforcement differ significantly than if the phrase were "I am going to do this to a child." The image may be illegal either way, but the context would help to prioritize it. Relatedly, law enforcement may assess that an image depicts adult genitalia, but context about the age of the recipient is important in assessing whether follow up action is needed. Reports that lack context are particularly challenging for non-U.S. law enforcement where there are many obstacles to obtaining additional information from platforms.[123]

In the process of reporting images, the occurrence of false positives—instances where non-CSAM images are mistakenly reported as CSAM—is inevitable. One officer told us that there are "a lot" of CyberTipline reports that are images of adults.[124] More false positives will mean fewer cases going unreported, and platforms must decide what balance they are comfortable with. False positives and false negatives can be minimized with better detection technology. One respondent criticized platforms for relying on their in-house technology. They perceived those as inferior to solutions offered by start-ups, suggesting that this choice might be driven by profit motives.[125] Platforms, however, might have reservations about using third-party services for screening potential CSAM due to legal and ethical considerations. An NGO employee highlighted platform concerns, asking, "Can we trust these organizations? What ethical due diligence have they done?"[126]

5.4 Information platforms receive from law enforcement

There are two types of information law enforcement could, in theory, provide to platforms related to their CyberTipline reports: the outcome of the report (for example whether it led to an arrest) and feedback about the quality of the reports (for example noting that a platform's reports are not being investigated because they only include login IP addresses and not upload IP addresses). In practice, platforms rarely get either piece of information from law enforcement.

Many trust and safety teams of both small and large platforms crave both types of information.[127] We spoke with staff at one platform which had only submitted about five tips in recent years. They manually review every tip, and said that they never received any follow-up from law enforcement, nor feedback about the quality of their tips. They found the lack of follow up somewhat distressing, particularly for one tip where they believed their platform was the only one where the content had been shared.[128] Some trust and safety employees say more

[123] Interview on February 27, 2024.
[124] Interview on August 18, 2023.
[125] Interview with an NGO employee on August 3, 2023.
[126] Interview on October 18, 2023.
[127] Interview with a platform employee on October 20, 2023; Interview with a platform employee on November 6, 2023.
[128] Interview with a platform employee on December 7, 2023.

outcome information would help them sell their work to executives and improve employee morale.[129]

Some platforms have proactively undertaken this effort themselves. One platform tracks whether they receive legal process from law enforcement based on their CyberTipline reports as a rough way to proxy whether law enforcement is investigating their tips. Another platform will reach out to law enforcement abroad to assess outcomes of their high priority reports.[130]

Some platform employees we interviewed had no issue with the status quo: "I don't need to know what happens once [the tips] go out the door. It would be nice to [hear] 'awesome report,' but I have so much to do. Thank you but I have to keep doing my work."[131] Similarly, another platform employee said they are okay with not knowing what happens to their tips, thinking it might be a "further invasion of privacy" to know more.[132]

There is a mechanism for law enforcement to submit feedback on reports. NCMEC has built into the report flow a way for law enforcement to submit outcome information in a structured format, which in turn would display general statistics about tips that have been closed back to the platforms. Law enforcement rarely provides this information, likely because law enforcement officers are overworked. "We are poor at communicating back outcomes," an investigator told us.[133] One respondent noted that there is a trade off between communicating back to platforms and investigating the next case.[134]

We heard some law enforcement officers complain about platforms requesting feedback on their tips. Some officers we interviewed felt that platforms knew what information law enforcement valued, and chose not to provide it. Our sense is that many smaller platforms are able and willing to change their processes but need precise feedback on how. Even larger platforms crave feedback from law enforcement on what makes reports more likely to be investigated, noting that the platform could make changes to its internal prioritization processes based on this information.[135] They added that they were aware that this could create Fourth Amendment tensions, but that "without that feedback you are stuck in a system where turning over anything is better than trying to think through how to do this well. Or the flip side is you bury your head in the sand."

Besides the lack of communication from law enforcement, platforms are also frustrated when reports are not investigated. A platform employee said they felt like their reports about multi-jurisdiction operations—which in their view are among their most important reports—were rarely investigated. "The system is not well set up to handle multi-jurisdiction cases," they said.[136] "We don't get the

[129] Interview with a platform employee on November 6, 2023.
[130] Interview with a platform employee on February 8, 2024.
[131] Interview with a platform employee on October 20, 2023.
[132] Interview with a platform employee on November 2, 2023.
[133] Interview with an investigator abroad on February 27, 2024.
[134] Interview with a platform employee who previously worked in law enforcement. Date of interview omitted to ensure respondent anonymity.
[135] Interview with a platform employee (date omitted to ensure respondent anonymity).
[136] Interview on March 6, 2024.

indication that the highest priority [reports] are getting worked even though we work nights and weekends to get them out the door ASAP."[137]

When platforms do hear from law enforcement about their reports, they share an additional set of frustrations. Sometimes they hear from law enforcement following up on a months-old search warrant that a platform never received because it was sent to an outdated fax number or email address. Platform employees sometimes feel that law enforcement lack an understanding of their platform and its various features and therefore do not know the most relevant data to request. Some platforms have law enforcement portals with detailed guides explaining what data can be requested and what the data means. Law enforcement will complain that these guides are not kept up to date.[138] Law enforcement may also be frustrated when platforms suddenly start requiring a warrant to disclose information for which they previously only required a subpoena.[139]

One former employee of a platform that submits many CyberTipline reports expressed frustration with how platforms are perceived and treated. They said there is a misperception that companies are trying to do the bare minimum with reporting requirements. They said they have heard this sometimes from NCMEC and frequently from Congress. These comments, they said, cause companies to get defensive: "Everyone should be rowing in the same direction, everybody wants the same result [...] companies aren't trying to monetize this stuff. [...] It's not like there's a lobbying group out there that's in favor of CSAM, everyone's on the same side." They perceived that the adversarial nature of interactions was a result of the fact that people need an enemy. It is not helpful if someone is in a meeting worrying that anything they say will be used against them.[140]

At the same time, we heard that platforms will get feedback about how to improve their reports, and then not incorporate the feedback.[141] One federal civil servant said there were frustrating conversations where a platform employee would suggest they could do something to change, but then (the civil servant perceived) their lawyers would stop them.[142] Our sense is that there is significant variation in how much effort platforms invest in creating actionable reports, and that the high-effort platforms find it frustrating when all platforms are grouped together.

Many platforms have law enforcement outreach officers, which both platforms and law enforcement cited as beneficial. The outreach person can respond to general law enforcement inquiries about, for example, figuring out what a variable means. One respondent said that law enforcement officers often do not understand how time consuming pulling data is for platforms, and that platforms may not understand that they could—when legally permissible—tell law enforcement "no." Instead, platforms would choose to just not engage with

[137] Follow-up interview on March 11, 2024.
[138] Interview with a law enforcement officer on August 18, 2023.
[139] Interview with a platform employee on October 20, 2023.
[140] Interview on October 6, 2023.
[141] Interview with NCMEC staff on November 2, 2023.
[142] Interview on October 24, 2023.

law enforcement, likely exacerbating tensions. Outreach officers can help with all of this.[143]

Platforms report being careful to avoid too close of a relationship with law enforcement. One platform employee, perhaps intentionally, does not have a law enforcement outreach officer, striving to be conservative in how their team engages with law enforcement because they have "seen it go sideways" when platforms get too close.[144]

5.5 Platforms identified by NCMEC for unactionable reports

NCMEC has markedly increased CyberTipline transparency in recent years. One of the ways they have done this is by publicly identifying platforms for which an overwhelming majority of their tips lacked sufficient location information for NCMEC to identify the appropriate law enforcement agency for referral. In 2022 NCMEC listed 36 platforms where at least 90% of the tips received were not actionable. We interviewed employees of several of the platforms on the list.

One platform admitted they deserved to be on this list. They had been automatically submitting many files that their AI tool incorrectly thought were CSAM.[145] NCMEC had reached out to them about this issue but the platform employee said that NCMEC's email was so kind they failed to understand the extent of the problem. It was only when they were informed more directly that they would be listed as a company whose tips "lacked actionable information" that they investigated what was going on.

The unactionable list included platforms that submitted a small number of total reports, meaning that just a small number of incomplete reports could put them over the 90% threshold. Two of the platforms we interviewed highlighted the fact that they submitted just one or two tips total, all of which lacked actionable information. One platform reported asking NCMEC three times for feedback on how to improve the actionability of their tips, and got no response.[146] 11 of the 36 platforms categorized in this way submitted six or fewer tips in 2022.

During conversations with NCMEC staff we suggested that platforms with very low reporting volumes might be excluded from this list. In their 2023 report, NCMEC has now adjusted their criteria to include only platforms that submitted at least 100 reports, of which at least 80% "lack substantive information."[147]

We should note that the platform perspective in this report is biased toward the platforms we interviewed. Platforms that were willing to be interviewed for this project are, at least to some extent, searching for, suspending, and reporting CSAM. Telegram is an example of an important platform that is not searching for CSAM. "Offenders tell very young kids to download Telegram," one respondent told

[143] Interview with a platform employee on October 20, 2023.
[144] Interview on November 6, 2023.
[145] Interview with a platform employee on November 2, 2023.
[146] Interview with a platform employee on November 27, 2023.
[147] NCMEC, "CyberTipline 2023 Report."

us.[148] In 2023 Telegram did not submit any CyberTipline reports, and Telegram's website boasts that "[t]o this day, we have disclosed 0 bytes of user data to third parties, including governments."[149]

5.6 Legal considerations for U.S. platforms

5.6.1 Platform caution and the Fourth Amendment

Platforms are well aware of the Fourth Amendment government agency and private search doctrines, as interpreted by *Ackerman*, *Wilson*, and other cases. Their desire to avoid government agency problems colors their interactions with state actors in both law enforcement and policy roles, and with NCMEC. On the receiving end of platforms' reports to the CyberTipline, the courses of action available to NCMEC and law enforcement are determined by the scope of platforms' private searches as communicated by the platforms.

We heard repeatedly that a positive, trusting relationship between platforms and governments is beneficial for child safety, but that there are legal reasons not to get too chummy. Platforms are rightfully leery of their child safety teams working so closely with law enforcement that they take direction from them rather than from the platform's legal team. Even if it comes from a good place, wanting to do everything they can to help law enforcement risks crossing a constitutional line, and platforms are aware that their conversations with law enforcement may come to light one day.[150] Multiple platform respondents told us that they are exceptionally cognizant of Fourth Amendment concerns and are extremely cautious in their interactions with law enforcement.[151]

In criminal prosecutions, platform personnel who submitted CyberTipline reports or otherwise communicated with law enforcement may see those communications disclosed in discovery and may be called upon to testify. This may involve written declarations, depositions, and testifying in pre-trial proceedings and at trial, over a time period that can span years.[152] Sometimes the reason is simply to have the platform employee authenticate evidence, but in some cases it is to determine whether, for Fourth Amendment purposes, the personnel acted on behalf of the platform or on behalf of law enforcement.

[148] Interview with a federal department employee on November 17, 2023.

[149] Telegram, "Telegram FAQ," 2024, https://perma.cc/52W6-6JNX.

[150] Interview with a platform employee on November 6, 2023.

[151] Interview with a platform employee on February 8, 2024.

[152] For example, the current Chief Information Security Officer at Yahoo, Sean Zadig, has supplied written and oral evidence in multiple CSAM cases dating back over a decade and across multiple employers. E.g., United States v. Drivdahl, 13-CR-18 (D. Mont. Mar. 6, 2014), https://perma.cc/675D-AM3Y; *Rosenow*, 50 F.4th at 730; United States v. Wolfenbarger, No. 16-cr-00519, 2019 U.S. Dist. LEXIS 213890, at *3 (N.D. Cal. Dec. 10, 2019), https://scholar.google.com/scholar_case?case=2079717243167991016. In the *Wolfenbarger* case alone, Zadig's email communications with law enforcement were disclosed in 2018 (as well as a written declaration he had submitted in *Rosenow*), he testified in two pre-trial hearings in July 2019, and he testified at trial in August 2021.

Unsurprisingly, platforms' lawyers appear to give that constitutional line a wider berth than their trust and safety teams might be inclined to do. One longtime federal civil servant said that her agency engages with platforms at the senior level, but the process is very bureaucratic. She'd like to work with the platforms to get 10 standard fields in CyberTipline forms, but she perceived that platforms' lawyers mess that up by invoking the Fourth Amendment. Even communicating specific data formatting problems to the platforms is "skirting the Fourth Amendment line." The government is limited to coming up with voluntary principles for reporting, which platforms are free to disregard even if they have nominally endorsed them.[153]

Avoiding law enforcement influence also manifests in a more technical context. Even before *Ackerman*, platforms (particularly very large ones) would only accept hashes from a hash value list that was compiled from non-NCMEC sources if the entity submitting the hash values promised the hashes did not come from law enforcement. *Ackerman* made platforms even more cautious about relying on hash values created by anyone other than NCMEC.[154] NCMEC is allowed by statute to supply hash values of known CSAM to platforms.[155]

Platforms decide whether to search for CSAM at all. Platform respondents emphasized to us that they are searching for CSAM of their own volition: "This is maybe the most egregious violation of our terms of service. Everyone finds this to be the worst of the worst, [finding and removing this content] is a business need," one platform employee said.[156] And for the most part, 18 U.S.C. § 2258A also lets platforms decide what information to include in their reports. Platforms are not required to have a human review the material being reported before submitting the CyberTipline report, but there are Fourth Amendment consequences riding on whether they do so and whether they convey that decision in the report.

5.6.2 The decision to view a file

The CyberTipline report form includes a box that the submitting ESP can check to indicate that a person at the platform opened each file being submitted in the tip; the exact language is "File Viewed by Company" (see Figure 5.3). Whether

[153] Interview with a federal civil servant on October 24, 2023. In March 2020, the United States, together with four other governments, jointly released a set of voluntary principles to counter CSEA, which 16 companies had endorsed by March 2022. U.S. Department of Homeland Security, "5 Country Ministerial Statement on the Second Anniversary of the Launch of the "Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse"," March 24, 2022, https://perma.cc/Z7V9-L6EJ.

[154] Interview with an NGO employee on November 6, 2023. Some platforms create their own hash values for CSAM they encounter on their service. E.g., *Wilson*, 13 F.4th at 964–65 (describing Google's process for assigning hash values to images and adding those values to its hash value repository).

[155] 18 U.S.C. § 2258C, https://www.law.cornell.edu/uscode/text/18/2258C. Section 2258C has not been a point of contention in CSAM cases the way Section 2258A has, though one district court did list 2258C's "authoriz[ation] [for] the hash value technology used in PhotoDNA" as one of the "circumstances" that it said other courts had found "sufficient to subject NCMEC's activities to Fourth Amendment requirements."*Coyne*, 387 F. Supp. 3d at 400 (citations omitted).

[156] Interview on February 8, 2024.

this box is checked has significant consequences. If it is checked, there is a strong argument that the private search doctrine (as interpreted by *Wilson* and *Ackerman*) has been satisfied, so neither NCMEC nor law enforcement need a search warrant to view that file—though it is prudent for investigators to get one anyway. However, the platform's decision about whether to do human review is not straightforward.

Two platforms whose employees we spoke to—one larger and one medium-sized—told us that they review all reports.[157] One of these employees said they do this because they want to make sure they are not sending NCMEC "junk,"[158] and the other similarly said they review media for all tips because they want to ensure the tips they are sending to NCMEC are high quality.[159] One interviewee said that platforms may have employees view content, but that they may not check the "File Viewed by Company" box because that part of the process has not been operationalized internally. There may also be cases where a submitter chooses not to check the box because a person reviewed the image, but not other aspects of the account that were preserved.[160]

Respondents from one platform noted that if content moderators are viewing a video, as soon as they observe CSAM they label the video as containing CSAM and stop watching the video, partly for moderator wellness reasons. The full definition of the "File Viewed by Company" box is "Did reporting ESP view entire contents of uploaded file?" In these cases the platform viewed only part of the file. The platform currently does not check the "File Viewed by Company" box; instead, it indicates that the moderator saw CSAM in the video through another part of the form, a free text entry box for providing additional information—but they are not sure if that is the optimal approach.[161] This respondent said they hope case law moves in the direction of confirming that viewing enough of the content to confirm that it contains CSAM is sufficient for NCMEC and law enforcement to then view the content without a search warrant. This example reflects the tradeoff between platform moderator well-being and CyberTipline efficiency, and illustrates the potential for ambiguity in the CyberTipline reporting form.

Many platforms do not take the approach of reviewing all tips, for multiple reasons. One is that the platform will know which of the images they are reporting are known images, and it may prefer not to expose employees to harmful content given that it already has high confidence that the content is CSAM that has already been viewed and reported before. An employee at a platform that takes this approach said: "We see each time an image is viewed as an independent harm to a child. Plus viewing the material is individually and cumulatively harmful [to moderators]. [It] burns out the people with expertise. [Additionally,] reviewing every image every time would make it impossible to review at scale."[162]

Certain platforms are known to check the file-reviewed box on the form when the

[157] Interview on October 20, 2023; Interview on November 6, 2023.

[158] Interview on October 20, 2023.

[159] Interview on November 6, 2023.

[160] Interview with an NGO employee on October 18, 2023.

[161] Interview with a platform employee on February 8, 2024.

[162] Interview on March 6, 2024.

file being reported was not opened but matches a hash value for CSAM that had been reviewed by a human previously, perhaps even years earlier. Yet that leaves law enforcement unsure whether the image being reported was reviewed this time[163]—and thus uncertain whether they need a warrant: some courts consider a hash match to previously-reviewed content sufficient to satisfy the private search doctrine, but *Wilson* did not.[164] The conservative approach is to always get search warrants, even if the box is checked, to reduce the risk of exclusion of the files in court.[165]

Platforms may also lack sufficient staffing to look at all of the tips they report. Many platforms choose to conduct full investigations for a subset of the tips they file, and provide extensive details for those in their CyberTipline report. These efforts are uniformly appreciated by law enforcement.[166] Some platforms may decide to only have humans view content that automated detection systems labeled as the worst of the worst, which is a tough decision to make[167] since it means reducing the quantity of CSAM an employee views, but increases the psychological harmfulness of the content they see. As noted above, the staffing issue can resurface in criminal prosecutions, as platform personnel may be required to spend time producing evidence, preparing declarations, getting deposed, and testifying in court, all of which takes them away from their primary job responsibilities.

Upon request NCMEC shared data with us on the percentage of reports sent to ICAC Task Forces where the platform had (or had not) viewed the files. Table 5.1 on the following page shows that among actionable reports sent to the Task Forces, which contained at least one file, the platform had not reviewed any of the files for 40% of these reports.

5.6.3 Platform information sharing around CSAM

Reviewing files is not the only point where the CyberTipline reporting process implicates user privacy. CSAM-related information-sharing across platforms came up in many interviews, with interviewees expressing a desire for greater information-sharing among platforms while also recognizing the privacy implications. Platforms can share some information with one another about bad actors on their respective services, but in practice they have historically shared less than the outer bounds that U.S. law would allow. Under the Stored Communications Act, platforms generally cannot disclose the contents of communications (such as an image file or the contents of an email) without the user's consent, but they

[163] Interviews with a federal department employee on November 2 & 17, 2023.

[164] *Wilson*, 13 F.4th at 978–79 (disagreeing with *Miller*, 982 F.3d at 429–30, and *Reddick*, 900 F.3d at 639); Interview with an assistant federal public defender on September 14, 2023 (discussing *Reddick*).

[165] Interviews with federal department employees on November 2 & 17, 2023.

[166] Interview with a law enforcement officer on September 22, 2023; Interview with an assistant district attorney on August 17, 2023.

[167] Interview with a former platform employee on October 6, 2023.

Table 5.1: For actionable reports with at least one file that NCMEC sent to ICAC Task Forces in 2023, percent of reports where the platform viewed the file. We are grateful to NCMEC for sharing this data with us.

Status	# of Reports	
Sent to ICAC Task Forces	908,762	
Sent to ICAC Task Forces that were actionable	670,491	
Sent to ICAC Task Forces that were actionable and contained at least one file	591,917	
		% of actionable reports w/ attachments
Sent to ICAC Task Forces that were actionable and contained at least one file, and where all reported files were indicated as viewed by ESP and/or publicly available	304,435	51.43%
Sent to ICAC Task Forces that were actionable and contained at least one file, and where some reported files were indicated as viewed by ESP and/or publicly available	50,031	8.45%
Sent to ICAC Task Forces that were actionable and contained at least one file, and where no reported files were indicated as viewed by ESP and/or publicly available	237,451	40.12%

may share non-content data.[168] That said, disclosing users' information still risks lawsuits,[169] and foreign laws (which may come into play if a platform incorrectly geolocates a user) may be less permissive than the SCA. Several interviewees said a clear legal safe harbor for information-sharing between platforms (akin to current protections for disclosing information to NCMEC)[170] would be helpful, though one added that there would need to be other positive incentives in place as well.[171]

One former platform employee opined that even without sharing content, platforms could collaborate to share other data, such as identifiers (e.g., email addresses), more than they have historically done. The SCA does not prohibit such sharing, and most platforms' privacy policies and terms of service would allow it.

[168] 18 U.S.C. § 2702(b), (c). "In other words, the Stored Communications Act generally precludes a [platform] from disclosing the contents of a communication, but permits disclosure of record information like the name, address, or client ID number of the entity's customers in certain circumstances."In re Zynga Privacy Litig., 750 F.3d 1098, 1104 (9th Cir. 2014), https://perma.cc/RY8R-9ADA.

[169] For example, one criminal defendant unsuccessfully sued Yahoo and Facebook under the SCA for disclosing information about him to NCMEC. Rosenow v. Facebook, Inc., 19-cv-1297, 2020 U.S. Dist. LEXIS 73513 (S.D. Cal. Apr. 27, 2020), https://perma.cc/JT9W-TNNF.

[170] 18 U.S.C. § 2702(b)(6); 18 U.S.C. § 2258B, https://www.law.cornell.edu/uscode/text/18/2258B.

[171] Interview with a platform employee on August 4, 2023; Interview with an NGO employee on October 18, 2023.

The trade-off is how to more effectively catch cross-platform bad actors without too much privacy intrusion.[172] Another interviewee observed that “it feels like a lose-lose” for platforms: if they don’t do enough information-sharing, they get critiqued; if they “do the gold standard,” they’re called too privacy-invasive.[173] The interviewee noted the need to “balance human rights [and] not overindex on this [CSAM] topic without other voices in the room” who have historically been adversely impacted by platforms’ policies and moderation choices. Recently, they said, there has been more engagement with sex-worker and LGBTQI+ groups, civil rights groups, and privacy groups to “invite them into the conversation.”[174]

One proposal we heard was to let multiple platforms collaborate to jointly submit a single report for a single bad actor that was “streamlined” and fleshed out with a lot of information.[175] That would result in fewer but higher quality reports to NCMEC, which currently receives multiple CyberTipline reports for accounts on multiple services that may all turn out to be held by the same individual. Increased cross-platform information-sharing is starting to become reality, though it has not yet reached the point of “batching” multiple platforms’ information into a single tip. The Tech Coalition facilitates information sharing about, for example, general approaches to detection.[176] In November 2023, while research for this paper was underway, the Tech Coalition launched Lantern, a “cross-platform signal sharing program” for platforms to share email addresses and usernames that may be associated with CSAM offenders.[177] This initiative can provide more CyberTipline reports and data about offenders who are using multiple platforms, and these offenders may be more likely to be doing hands-on offenses than other offenders. For example, imagine a social media platform discovers a user who shared a CSAM image. By sharing the username for that individual with the Lantern project, another platform searches the username and discovers that the individual is contacting children on their platform.

Criminal defense attorneys, however, were more critical of the idea of increased information-sharing between platforms. A former assistant federal public defender said they would be deeply uncomfortable with platforms collaborating on reports, even for non-content information such as usernames and IP addresses. “Do we really want that level of privacy intrusion? I don’t, as a user.”[178] They and other interviewees also flagged reliability and accuracy concerns. If platforms are “actively collaborating” to compile a CyberTipline report, another assistant federal public defender said, then “it’s almost like tech companies are vigilantes at that point, going out and hunting down people and gathering dossiers on them to assist law enforcement.” If they made errors (which happens already), that would open them up to liability: platforms would be getting their own users put in

[172] Interview with a former platform employee on October 6, 2023.
[173] Interview with an NGO employee on October 18, 2023.
[174] Interview with an NGO employee on October 18, 2023.
[175] Interview with a platform employee on August 4, 2023.
[176] “What We Do,” The Technology Coalition, https://www.technologycoalition.org/what-we-do.
[177] Sean Litton, “Announcing Lantern: The First Child Safety Cross-Platform Signal Sharing Program,” The Technology Coalition, November 7, 2023, https://www.technologycoalition.org/newsroom/announcing-lantern.
[178] Interview with a former assistant federal public defender on August 24, 2023.

jail "based on a bad package of information."[179] Another former criminal defense attorney said they would have no problem with more efficient reporting, but called accuracy the main consideration. If there is a high level of inaccuracy, then bundling reports together to streamline them would just mean "roping more innocent people into the net" and handing them to law enforcement.[180] That inaccuracy could happen, for example, where a service lets new users register for an account without verification. If bad actors create accounts using someone else's email, innocent users might get ensnared when platforms share bad actors' supposed email addresses with each other.[181]

Privacy and reliability concerns, together with legal risk, help to illuminate why platforms have historically limited their information sharing. That said, participants in the new Lantern program are ostensibly comfortable with sharing more, or at least streamlining the sharing of information generally already considered okay to share.[182] There are still benefits to the more conservative approach. While there is an appetite among platforms to share concrete, case-specific information in addition to their current discussions of law, policy, and practices,[183] still even those more high-level discussions can be surprisingly candid when they are in a confidential, high-trust environment of vetted participants. Overall, information sharing helps platforms' child safety teams improve their resilience and feel less alone; one respondent said: "You feel you're part of a bigger community, which is powerful."[184]

[179] Interview with an assistant federal public defender on August 18, 2023. This "vigilante" framing also raises a Fourth Amendment government agency issue.

[180] Interview with a former criminal defense lawyer on October 4, 2023.

[181] Interview with an assistant federal public defender on August, 18, 2023.

[182] Interview with a platform employee on March 11, 2024. The same respondent highlighted another barrier to information sharing: companies may want to avoid being labeled as having a child safety problem, and may also fear that sharing information would reveal that their technology is outdated.

[183] Interview with a platform employee on August 4, 2023; Interview with an NGO employee on October 18, 2023.

[184] Interview with an NGO employee on October 18, 2023.

6 Findings: NCMEC

Key findings

- NCMEC has enhanced their deconfliction work—the process of linking reports to avoid overlapping investigations by multiple agencies—but there are areas for improvement.
- NCMEC is in the process of tagging old files to automatically identify similar new reports through hash values, even when the files themselves cannot be accessed.
- NCMEC staff are frequently poached by industry.
- NCMEC's inability to use cloud services for storing CyberTipline data slows down potential technological advancements, but reasonable people disagree as to whether CyberTipline data should leverage cloud services.
- Progress in technical updates to the CyberTipline is often gradual, and these updates may be underutilized by platforms once implemented.
- Law enforcement agencies use a variety of interfaces to process CyberTipline data, each with its own set of advantages and drawbacks.
- The preferences of law enforcement agencies vary; some want NCMEC to label one type of report as "actionable," while others want the same type of report labeled "informational."
- The *Ackerman* ruling of 2016 significantly altered NCMEC's operations. They choose to no longer open files not reviewed by the reporting platform, which hampers their ability to swiftly identify new victims and label reports with memes or viral content.
- Fourth Amendment concerns have also limited NCMEC's ability to tell platforms directly and at scale what makes a CyberTipline report actionable.

When NCMEC receives a report, their first step is to determine the appropriate jurisdiction for forwarding it. This determination relies on multiple CyberTipline report fields.[185] Generally, for most countries and the majority of tips, NCMEC automatically forwards these tips without conducting any initial analysis. For reports staying within the U.S., the relevant law enforcement agency—usually an ICAC Task Force or federal agency—is identified for receipt.[186] Many reports where the file is part of a known series are forwarded to law enforcement within minutes. Other reports are put into a queue for NCMEC analysts, prioritized based on variables including whether there is information about a victim. These reports are typically sent to law enforcement within a few days.[187]

[185] Interview with NCMEC staff between January 30 and February 1, 2024.

[186] NCMEC notes that the relatively small number of ICAC Task Forces benefits this referral process. For their work on missing children they must interact with many more local law enforcement agencies. (Interview between January 30 and February 1, 2024.)

[187] Interview with NCMEC staff between January 30 and February 1, 2024.

6.1 Deconfliction

One of NCMEC's key roles is "deconfliction," a term used by both NCMEC and law enforcement to describe the process of linking reports to avoid multiple law enforcement agencies investigating the same case. Deconfliction is achieved through at least four methods. First, NCMEC employs a partially automated approach to search for matches in CyberTipline reports across various entity fields, such as email addresses or IP addresses. An analyst reviews the matches to assess whether they are meaningful; for example, thousands of matches to a generic and likely made-up email address may not be meaningful. Law enforcement began seeing linked reports based on the automated entity matching system in 2021,[188] marking a significant advancement from the previous lack of automated matching.

Second, analysts manually copy and paste information to search for matches with previously filed tips. In cases where a match is found, either through automated or manual processes, the law enforcement report will indicate an entity match with another CyberTip, including the relevant tip number.

Third, as of the end of 2023, U.S. law enforcement agencies have the capability to independently search identifiers in NCMEC's database to determine if the identifier has been mentioned in other NCMEC CyberTipline reports.[189] This feature was a common request in numerous interviews we conducted in 2023. Prior to this rollout, law enforcement could search an identifier and discover if it appeared in an earlier report, but they lacked visibility into the specific field where an identifier—such as an email address—appeared in a report. Knowing whether an email address was listed as a sender or receiver is important because investigating a sender of CSAM is often a higher priority, given that recipients might receive such materials unwillingly. Our assessment is that NCMEC requests and receives feedback for these types of features frequently, but is resource constrained when it comes to developing and implementing the features.

Fourth, law enforcement can provide identifiers to NCMEC to conduct the search and report back findings. Law enforcement report that NCMEC responds to these requests very quickly—sometimes within the hour, and usually within the day.[190] NCMEC is uniquely positioned for effective deconfliction due to their access to cross-platform and cross-jurisdiction data, and insights from both platform reports and reports from the public. Nonetheless, platforms and law enforcement can do their own deconfliction as well.

This deconfliction system faces certain limitations. Errors in completing the CyberTipline form can hinder the automated entity matching process. Supplemental materials provided by platforms are not automatically scanned for potential matches. More advanced deconfliction methods exist that remain unused; these could be particularly useful in investigating large scale organized crime networks. One respondent provided an example of a case involving sextortion traced back

[188] Interview with NCMEC staff between January 30 and February 1, 2024.
[189] Interview with NCMEC staff between January 30 and February 1, 2024.
[190] Interview with a law enforcement officer on December 15, 2023.

to Nigeria, where offenders frequently employed similar tactics but used unique usernames and email addresses. Grouping these cases by tactics could ensure just one agency in Nigeria gets these tips, preventing nationwide duplication of efforts.[191] While individual platforms could conduct such analysis, they lack insight into activities on other platforms that might be linked to the same criminal network. Law enforcement agencies, limited to the tips they receive, face similar constraints. An organization like NCMEC or a comparable regional entity outside the U.S. would be ideally positioned for this task, but such report grouping is not currently in practice.

Improvements to the entity matching process would improve CyberTipline report prioritization processes and detection, but implementation is not always as straightforward as it might appear. The current automated entity matching process is based solely on exact matches. Introducing fuzzy matching, which would catch similarity between, for example, bobsmithlovescats1 and bobsmithlovescats2, could be useful in identifying situations where a user, after suspension, creates a new account with an only slightly altered username. With a more expansive entity matching system, a law enforcement officer proposed that tips could gain higher priority if certain identifiers are found across multiple tips.[192] This process, however, may also require an analyst in the loop to assess whether a fuzzy match is meaningful.

It is common to hear of instances where detectives received dozens of separate tips for the same offender.[193] For instance, the Belgium Federal Police noted receiving over 500 distinct CyberTipline reports about a single offender within a span of five months.[194] This situation can arise when a platform automatically submits a tip each time a user attempts to upload CSAM; if the same individual tries to upload the same CSAM 60 times, it could result in 60 separate tips. Complications also arise if the offender uses a Virtual Private Network (VPN); the tips may be distributed across different law enforcement agencies. One respondent told us that a major challenge is ensuring that all tips concerning the same offender are directed to the same agency and that the detective handling them is aware that these numerous tips pertain to a single individual.[195]

There are a number of explanations for why two reports about the same offender could get sent to different jurisdictions, including that the deconfliction process is imperfect. A key challenge, however, is that law enforcement use a variety of interfaces to manage CyberTipline reports. With funding from OJJDP and Meta, NCMEC created a Case Management Tool for law enforcement that allows investigators to filter reports by platform and many other variables.[196] The tool clearly visualizes whether a report is linked to other reports through entity matches. The Case Management Tool is used in many countries, but not all, and in the U.S. only a handful of Task Forces use the Case Management Tool as their

[191] Interview with an NGO employee on October 10, 2023.
[192] Interview on August 18, 2023.
[193] Interview with a federal department employee on November 2, 2023.
[194] The AviaTor Project, "Save Time, Save Lives."
[195] Interview with a federal department employee on November 2, 2023.
[196] NCMEC, "CyberTipline 2022 Report."

primary way of working through CyberTipline reports.[197] Most ICAC Task Forces use the ICAC Data System, a tool that preceded the Case Management Tool. The ICAC Data System has a number of advantages: (1) it allows for deconfliction between CyberTipline reports and other Task Force cases that come in from other investigative work; (2) it has a number of practical features for law enforcement related to, for example, reimbursement processes; and (3) law enforcement agencies have used it for longer and are more familiar with the interface. The incumbent advantage is significant: both tools are provided to Task Forces free of charge, so changing to NCMEC's tool would incur significant switching costs without any corresponding savings on budget. As best we can tell, however, the ICAC Data System does not visualize report linking in the same way that the Case Management Tool does, and it (like other tools) lacks the customization capabilities of the NCMEC tool.[198]

NCMEC is currently undertaking an exhaustive review of all files ever submitted to the CyberTipline and when complete, this review should help law enforcement triage reports. In a process that began during the COVID-19 pandemic, NCMEC staff are coding a de-duplicated set of all viewable submitted files going back to 1998, and enriching them with a number of more recently added pieces of metadata, including whether they are memes or viral. This process requires multiple NCMEC employees to independently code every file. Once complete, if NCMEC receives a report with a file they are not allowed to open, they will sometimes be able to assess from the hash whether it is a file they have previously viewed, and if so, link the report to a viewable file that would help law enforcement triage. This labeling process will also reduce future NCMEC staff exposure to known CSAM.[199]

Alongside deconfliction, NCMEC sometimes conducts a manual investigation of a report before forwarding it to law enforcement. This investigation, potentially including open-source investigation, serves dual purposes: first, it aids in determining the appropriate jurisdiction for the tip, especially when an IP address is not provided. Second, it can supply valuable information to law enforcement. However, opinions on the usefulness of this analysis are divided. A law enforcement officer considered it of limited utility, pointing out that NCMEC lacks access to the databases available to law enforcement: "All we need is a phone number and a name," the officer said.[200] While some of NCMEC's analysis is good, the officer said their team would likely need to replicate the analysis.

We shared this observation with NCMEC, and they offered three responses. First, NCMEC noted that one goal of their open source review is to geolocate the tip for accurate triage. They believe that any relevant information found through that investigation should be shared and not withheld.[201] Second, they said that

[197] Interview with NCMEC staff between January 30 and February 1, 2024.

[198] Interview with a law enforcement officer on February 5, 2024. Law enforcement agencies that do not use the Case Management Tool may still use NCMEC's law enforcement portal to look up CyberTipline reports and do their own deconfliction. (Interview with NCMEC staff between January 30 and February 1, 2024.)

[199] Interview with NCMEC staff between January 30 and February 1, 2024.

[200] Interview on August 25, 2023.

[201] Interview with NCMEC staff on November 13, 2023.

their open source review supports efforts to prioritize reports. Third, they said that a general challenge they face is meeting the heterogenous needs of diverse law enforcement agencies. Our interviews were biased toward the perspective of law enforcement experienced in investigating online child exploitation. It may very well be the case that the initial manual investigations NCMEC conducts are useful for law enforcement agencies with less experience investigating cyber crimes, crimes against children, or CyberTipline reports. NCMEC allowed us to observe their open-source investigation report protocols. We observed—and NCMEC agreed—that some custom-built tooling could make this process more efficient.[202]

Diverse law enforcement preferences pose a significant challenge for NCMEC: they noted that they share tips with dozens of agencies in the U.S. alone, each with different preferences for what they want in the reports. NCMEC said they conducted a workshop with the goal of seeking alignment on what ICAC Task Forces want from NCMEC, and instead the workshop highlighted the diversity of opinion.[203] And this is just within the U.S.; another country might want certain types of tips labeled actionable that a Task Force only wants as informational (or vice versa).[204] While the Case Management Tool would allow Task Forces to filter on many of the variables they care about, as noted above most Task Forces are not using this as their primary report interface. NCMEC is in the process of customizing how they process reports for various jurisdictions, so that one Task Force could receive a report as "informational" while another Task Force could receive a similar report as "actionable."[205]

6.2 The CyberTipline and technology

While numerous respondents acknowledged significant advancements in NCMEC's technological capabilities over time, there remains a perception that "NCMEC has stood still in time a little bit."[206] NCMEC faces unique constraints in updating the CyberTipline, including resource constraints, limitations on usable third party products, accommodating law enforcement processes, and balancing upkeep with innovation. This situation was metaphorically described by a federal department employee: "The house is flooding, they're bailing water, and we're asking them to build a drainage system at the same time. You can't stop bailing, otherwise you'll drown."[207] One respondent indicated that engineering tasks that appear to be straightforward might take NCMEC a while to complete.[208]

Two respondents noted that there is a need to update the CyberTipline reporting schema. A suggested upgrade from our interviews was to add a box where platforms can indicate whether their tip may contain AI-generated CSAM. By the

[202] Interview with NCMEC staff between January 30 and February 1, 2024.
[203] Interview with NCMEC staff on November 2, 2023.
[204] Interview with NCMEC staff on November 13, 2023.
[205] Interview with NCMEC staff between January 30 and February 1, 2024.
[206] Interview with a platform employee on October 20, 2023.
[207] Interview on November 17, 2023.
[208] Interview with an NGO employee on October 18, 2023.

time of our visit to NCMEC the generative AI box had been added (see Figure 5.3 on page 26), but there is a sense that something like this takes far longer to complete than it would take in industry.[209] One respondent described a process where NCMEC will eventually make iterative improvements to reporting fields that platforms proceed to ignore, providing no positive reinforcement for such effort: "There's no incentive [for NCMEC to ensure the process] is a well-oiled machine because industry doesn't take advantage of new fields."[210]

Several factors may contribute to this. First, NCMEC operates with a limited budget and as a nonprofit they may not be able to compete with industry salaries for qualified technical staff. The status quo may be "understandable given resource constraints, but the pace at which industry moves is a mismatch with NCMEC's pace."[211] Additionally, NCMEC must also balance prioritizing improving the CyberTipline's technical infrastructure with the need to maintain the existing infrastructure, review tips, or execute other non-Tipline projects at the organization. Finally, NCMEC is feeding information to law enforcement, which work within bureaucracies that are also slow to update their technology. A change in how NCMEC reports CyberTipline information may also require law enforcement agencies to change or adjust their systems for receiving that information.

NCMEC also faces another technical constraint not shared with most technology companies: because the CyberTipline processes harmful and illegal content, it cannot be housed on commercially available cloud services. While NCMEC has limited legal liability for hosting CSAM, other entities currently do not, which constrains NCMEC's ability to work with outside vendors.[212] Inability to transfer data to cloud services makes some of NCMEC's work more resource intensive and therefore stymies some technical developments. Cloud services provide access to proprietary machine learning models, hardware-accelerated machine learning training and inference, on-demand resource availability and easier to use services. For example, with CyberTipline files in the cloud, NCMEC could more easily conduct facial recognition at scale and match photos from the missing children side of their work with CyberTipline files. Access to cloud services could potentially allow for scaled detection of AI-generated images and more generally make it easier for NCMEC to take advantage of existing machine learning classifiers. Moving millions of CSAM files to cloud services is not without risks, and reasonable people disagree about whether the benefits outweigh the risks. For example, using a cloud facial recognition service would mean that a third party service likely has access to the image. There are a number of pending bills in Congress that, if passed, would enable NCMEC to use cloud services for the CyberTipline while providing the necessary legal protections to the cloud hosting providers.

Numerous organizations are eager to assist NCMEC with technological advance-

[209] Interview with an NGO employee on October 18, 2023; Interview with a platform employee on October 20, 2023.

[210] Interview with a former platform employee on December 20, 2024.

[211] Interview with an NGO employee on October 18, 2023; Interview with a platform employee on October 20, 2023.

[212] 18 U.S.C. § 2258D, https://www.law.cornell.edu/uscode/text/18/2258D.

ments, yet NCMEC faces challenges in utilizing this external support.[213] We heard both from NCMEC and a separate respondent that NCMEC commissioned an API that facilitates the matching of CyberTipline report IP addresses with data from peer-to-peer file-sharing sites. A match would indicate that the IP address was not just associated with (for example) a single image upload as indicated on the tip, but that it was also associated with CSAM uploads or downloads on file-sharing sites. If law enforcement had two single-image upload tips, one with a match to a peer-to-peer file-sharing site and one without, that would suggest that they should prioritize investigating the former. This type of API would appear to fill a clear need from law enforcement officers who want to be able to more accurately triage tips. The API was completed in fall 2020, but NCMEC has yet to integrate it into their systems.[214]

Similarly, NCMEC told us that Google has offered Google Cloud services to assist with CyberTipline language translation to make it easier for law enforcement abroad to investigate tips. Yet NCMEC has not been able to accept this offer in part due to the engineering resources required for implementation, but also due to the care and processes that would need to be invested to mitigate risks of inaccurate translations. The challenge for NCMEC is not only about technically integrating new APIs; it also involves ensuring that these tools do not misuse their extremely sensitive data. NCMEC also notes that for the moment this has taken a backseat to domestic issues that need to be addressed.[215]

Several platform employees expressed a desire for NCMEC to offer detailed briefings on emerging tactical trends in online child exploitation specifically tailored to trust and safety staff who specialize in child exploitation issues. Most of NCMEC's existing training is geared towards individuals new to the field. However, one respondent said that NCMEC might not have the resources to fully utilize its data and provide real-time insights into trends.[216]

6.3 Perspectives on NCMEC

A majority of law enforcement respondents perceived NCMEC as doing their best given their limited resources, constrained mandate, and the restrictions imposed by the Fourth Amendment. An officer expressed high regard for NCMEC, stating, "NCMEC does a great job with a lot of things. Their challenge is they are a conduit. They aren't law enforcement, they don't have the stuff we have," referring specifically to police databases.[217] They added: "I don't hold anything but the highest respect for NCMEC. [NCMEC staff] don't have authority to do more than what they do." Another officer praised the value of having a single clearinghouse, and that their longevity and dedication is an asset.[218] They drew a parallel between NCMEC and a police dispatch commander, noting that while police officers often

[213] Interview with an NGO employee on November 6, 2023.
[214] Interview with NCMEC staff on November 13, 2023; Interview on December 5, 2023.
[215] Interview with NCMEC staff on November 13, 2023.
[216] Interview on March 6, 2024.
[217] Interview on August 18, 2023.
[218] Interview on August 25, 2023.

get frustrated with their dispatcher, it is important to remember, "You can't shoot the messenger."

Many current and former platform employees felt similarly. A former platform employee remarked, "most companies look at NCMEC and are pretty happy that it exists."[219] By forwarding reports on to law enforcement, they added, NCMEC plays a crucial role in disrupting CSAM production and distribution networks. This aligns with the interests of platforms, which aim to keep CSAM off their sites for business reasons. A healthy and efficient NCMEC reporting system is in companies' interests, he said. Another platform employee noted that having a single clearinghouse with a system for escalating urgent cases, including clear points of contact, increases efficiency.[220]

NCMEC also alleviates the pressure foreign governments might otherwise levy on platforms. This applies particularly to cases where such pressure might be viewed as normatively undesirable, such as requests from authoritarian regimes that could violate user privacy. The presence of the CyberTipline allows platforms to direct foreign law enforcement to work through their government's U.S. legal attaché, ensuring access to information shared with NCMEC. According to one respondent, this approach helps reduce the burden on platforms to take actions that could potentially harm user privacy.[221]

Some respondents had less favorable opinions of NCMEC. One described the organization as arrogant and difficult,[222] a viewpoint possibly influenced by the respondent's work in law enforcement advocacy; both NCMEC and Task Forces may perceive that they compete for the same financial resources. Legally and practically, NCMEC has a monopoly on the work that they do. There is a sense that perhaps this is how it must be, but that this may have fostered certain undesirable behaviors. A number of respondents feel that NCMEC is disincentivized to reduce the number of CyberTipline reports, suggesting that a higher number of tips could be used by NCMEC to justify requests for more funding.[223] While it is accurate that NCMEC references the growing number of CyberTipline reports to underscore their need for more resources,[224] this does not necessarily indicate that their incentives are misaligned. In fact in our interviews with NCMEC employees we saw evidence of the opposite: for example, they recounted an instance where they informed a platform that reported a high volume of tips that many of their tips were of a meme that did not meet NCMEC's classification for CSAM. This type of conversation could have the effect of reducing the overall number of CyberTipline reports.

In a discussion with a non-U.S. NGO, we broached the subject of NCMEC potentially requiring additional resources for enhancing its technical infrastructure. The respondent was aghast at the thought of NCMEC receiving more funding:

[219] Interview on September 22, 2023.
[220] Interview with a platform employee on March 6, 2024.
[221] Interview with a former platform employee on September 22, 2023.
[222] Interview with a lobbyist on October 20, 2023.
[223] Interview with a lobbyist on October 20, 2023.
[224] Interview with NCMEC staff on November 2, 2023.

"NCMEC is at the top of the pyramid, they are the king of the castle," the respondent said, adding that NCMEC was not fully meeting the duties that come with such a position. The respondent believed that NCMEC should first increase accessibility for academic researchers to examine their data and engage more actively with civil society before receiving additional funds. They emphasized, "If NCMEC is going to make a meaningful contribution to the global online harms ecosystem, it has to be more collaborative."[225] We note that NCMEC staff provided exceptional transparency for our project, participating in several lengthy interviews and allowing us to observe their work at their headquarters for three days.

We repeatedly heard from respondents that NCMEC might be trying to do too much. At the same time, it was not always clear to us if respondents were aware that Congress mandates or authorizes (depending on a reader's perspective) most of NCMEC's activities.[226] Congress states that annual grants to NCMEC "shall" be used to operate a missing child hotline, operate a clearinghouse for missing and exploited children, along with 13 other programs and services. Still, one respondent believed that NCMEC offers a range of unmanaged services with insufficient quality control.[227] "NCMEC can never say no. They always want to do everything, so a lot of stuff falls through the cracks," one respondent said. "At least they are trying."[228] This respondent perceived that NCMEC's priorities "change quarterly based on who is cutting them a check. They get a lot of projects 60-80% done, shelve them for a few years, then come back to it."

We asked NCMEC what they would do with more resources, and they highlighted the need to build out their technology team to accelerate progress on their technological roadmap. NCMEC also pointed out that there is a "never ending cycle of trying to replace the workforce," considering the NGO-level salaries for analysts, and the fact that industry is constantly poaching their analysts.[229] During our interviews for this project, we frequently noticed that many trust and safety professionals in industry who specialize in addressing child sexual exploitation issues had previously been employed by NCMEC.

A few critiques were voiced regarding NCMEC's perceived relationship with law enforcement. While NCMEC is exceptionally careful about not demanding information from platforms, two former law enforcement respondents observed that NCMEC occasionally behaves as if law enforcement were their subordinates, for example asking law enforcement for information about a case. "We know what we are doing, and NCMEC is calling and saying 'we need this, we need that.' No you don't. We will get you all that after the [rescued] kid is sitting in our car."[230] Law enforcement may be confused about whether they are in fact obligated to respond to such requests, not understanding whether NCMEC has authority over them. One respondent mentioned that during NCMEC's training sessions with ICAC Task

[225] Interview on December 5, 2023.
[226] 34 U.S.C. § 11293, https://www.law.cornell.edu/uscode/text/34/11293.
[227] Interview with an NGO employee on October 18, 2023.
[228] Interview with an NGO employee on November 6, 2023.
[229] Interview with NCMEC staff on November 13, 2023.
[230] Interview with a platform employee on October 20, 2023.

Forces, they advise prioritizing CyberTipline reports above other investigations, which the respondent deemed inappropriate.[231]

Last, we note that NCMEC does important victim identification work that frequently intersects with the CyberTipline. NCMEC analysts often immediately know whether an image is part of a known series or if it represents a new victim requiring identification.[232] This aspect of NCMEC's work received widespread praise from respondents. While our research did not focus on this aspect of the CyberTipline, many of the challenges discussed have implications for victim identification. For instance, when a platform submits a tip without checking the "File Viewed by Company" box, NCMEC's inability to immediately access the file can result in delays in identifying victims.

6.4 Legal considerations for NCMEC

6.4.1 Changes in NCMEC practices post-*Ackerman*

Fourth Amendment issues are particularly salient for NCMEC, which *Ackerman* found is part of the government for Fourth Amendment purposes.[233] NCMEC disagrees with that decision, which was "painful" for its employees. In their eyes, the case reflects confusion about NCMEC having an investigative role when it's merely a middleman.[234] However, NCMEC works on incoming tips before passing them to law enforcement, such as by deconflicting and geolocating reports and determining if a reported file is publicly available on social media.[235] NCMEC declined to call those activities "investigative" since they're based on open-source data, and rejected the suggestion that they might contribute to the perception that NCMEC has an investigative role. Still, NCMEC won't flout the *Ackerman* decision, as that would risk undermining individual cases and damaging the organization. That is, although NCMEC now takes pains to underscore its private nonprofit status in its messaging,[236] it conducts its work as though it were a government actor to comply with court rulings.

Operationally, after the *Ackerman* decision in 2016, NCMEC stopped its practice of opening reported files that hadn't been viewed by the platform.[237] The "File Viewed by Company" checkbox was added to the CyberTipline form at the start of

[231] Interview with a lobbyist on October 20, 2023.
[232] Interview with NCMEC staff on November 13, 2023.
[233] *Ackerman*, 831 F.3d at 1295–308.
[234] Interview with NCMEC staff on December 14, 2023.
[235] Interviews with NCMEC staff on November 2, 2023; Interview with NCMEC staff on December 14, 2023.
[236] Interview with NCMEC staff on December 14, 2023.
[237] Interview with NCMEC staff on November 13, 2023. This only applies to CyberTipline reports that will be sent to U.S. law enforcement. NCMEC is able to open files, even if the "File Viewed by Company" box is not checked, if the report will be sent to non-U.S. law enforcement (interview with NCMEC staff between January 30 and February 1, 2024).

2014. The report at issue in *Ackerman* was a pre-2014 report that did not contain this box.[238]

Government agency doctrine has affected NCMEC's work both internally and externally. Multiple interviewees expressed frustration with NCMEC's reticent attitude post-*Ackerman*. One interviewee said NCMEC's fear of being deemed a state actor "has really overtaken" some of its core data collection, preservation, evaluation, and vetting duties. It behaves as a pass-through "conduit" for fear of corrupting an investigation if it does something more (such as viewing material, triage, or deduplication). NCMEC is "not a fish or a fowl," they said; "it's a precarious situation."[239] Another interviewee thought that as a result of the *Ackerman* decision NCMEC feels "hamstrung" from participating more fully in addressing the CyberTipline reporting process's shortcomings.[240]

One consequence of this "pass-through conduit" approach is the impact on the quality of reports to law enforcement. The "Fourth Amendment conundrum" is that platforms and NCMEC alike "domino" reports down the line to law enforcement.[241] Platforms kick the can down the road to NCMEC to reduce risk; they view it as safer to overreport, even for viral memes,[242] which both NCMEC and law enforcement consider "informational" rather than "actionable." But if a file was not reviewed by the platform, then NCMEC cannot open it and see whether it is a viral meme. What's more, not every platform uses the "Potential Meme" checkbox on the CyberTip consistently or at all.[243] Thus, if a platform reports a viral meme without checking the "reviewed by platform" or "meme content" boxes, NCMEC will send the report to a Task Force as potentially "actionable" but without further context.[244] The Task Force officer may then go through the effort of obtaining a warrant only to discover that the file is a meme. Had the platform checked the "reviewed" box or the "meme" box, NCMEC would have been able to review the content and forward it as "informational."

Another consequence of *Ackerman* is that in NCMEC's communications with platforms, it takes care to avoid government agency issues, which some platform respondents perceived came at the expense of clarity about how to submit a high-quality CyberTipline report. By its own admission, NCMEC lacks authority to make platforms change their reporting, so when platforms ask what would make a CyberTipline report "more robust," NCMEC will respond by giving options and citing examples of what other companies report.[245] As experienced on the platform side, one platform said that government agency case law had caused significant "collateral damage."[246] Another platform said that when responding to platform inquiries, NCMEC will not guide or advise them on whether to report

[238] Interview with NCMEC staff on December 14, 2023; Interview with NCMEC staff on January 30, 2024.
[239] Interview with an attorney for victims on October 12, 2023.
[240] Interview with a lobbyist on October 20, 2023.
[241] Interview with an attorney for victims on October 12, 2023.
[242] Interview with a platform employee on December 20, 2023.
[243] Interview with NCMEC staff on November 13, 2023.
[244] Eid.
[245] Interview with NCMEC staff on December 14, 2023.
[246] Interview with a platform employee on December 20, 2023.

certain material or what to do to make reports more actionable, and will not answer whether something that one platform is seeing is a trend happening at other platforms as well.[247]

The CyberTipline form does not inherently lend itself to high-quality reporting. Calling the form "robust," NCMEC noted that it provides a lot of fields to fill in while acknowledging that nobody fills out every single field. All of the form fields, a NCMEC representative said, were requested by either law enforcement or platforms. When asked how platforms are supposed to know which fields are the most important to fill in (since NCMEC will not tell them directly), NCMEC responded that "it's not that hard to know what might be most helpful. [...] It's not terribly complicated."[248] By contrast, one platform employee told us that "it takes a decent amount of real world understanding" to know which report fields are important. For example, the report has a time zone field to accompany the incident time, which is a critical field for law enforcement, but many platforms do not know it is important and so do not use it.[249]

Upon learning that NCMEC gives platforms guidelines for filling out reports in customized CyberTipline onboarding trainings, we asked NCMEC why they do not write those guidelines down. They told us that if they had a written document, defense attorneys would characterize this in criminal cases as "NCMEC is advising companies what to report." NCMEC found it preferable for best practices to come from the Tech Coalition, which is composed solely of private companies, rather than NCMEC. Nevertheless, NCMEC conceded that although defense attorneys would seize upon it for a "platforms are agents of the government" argument, NCMEC could be more vocal about the core top-priority fields to complete in the form, and then platforms could take that guidance or leave it.[250]

The specter of the Fourth Amendment even hovers over various documentation provided by NCMEC. The footer of the NCMEC Case Management Tool software (used by law enforcement agencies) includes language stating that NCMEC is "a non-profit 501(c)(3) organization [...] not an agent or instrumentality of the government or law enforcement agency[,] and does not act in the capacity of or under the direction or control of a government or law enforcement agency." The same language appears at the bottom of the CyberTipline reports submitted to law enforcement. Similarly, the CyberTipline reporting API starts with an underlined disclaimer,[251] perhaps for fear that NCMEC's merely giving usage instructions might be construed as a governmental entity telling platforms what to report.

That said, NCMEC is comfortable being in the role of providing feedback from law enforcement to platforms about their reports in an "information sharing" manner.[252] NCMEC disintermediates itself by hosting biannual roundtables that

[247] Interview with a platform employee on November 6, 2023.
[248] Interview with NCMEC staff on December 14, 2023.
[249] Interview with a former platform employee on December 20, 2023.
[250] Interviews with NCMEC staff on January 30 and 31, 2024.
[251] "CyberTipline Reporting API Technical Documentation," (*"While ESPs have a statutory duty to report apparent child pornography to NCMEC's CyberTipline (see 18 U.S.C. § 2258A), the reporting of data via the web service, other than the incident type and date/time of incident, is voluntary and undertaken at the ESPs' initiative."*)
[252] Interview with NCMEC staff on December 14, 2023.

bring law enforcement and select participating platforms together to discuss CyberTipline reporting,[253] as a means of opening the lines of communication so that platforms can hear from law enforcement directly.[254] These roundtables appear to serve an important function: other contexts, such as meetings between federal agency officials and platform lawyers, seem not to be conducive to open and effectual communication.[255]

6.4.2 Changes in NCMEC practices post-*Wilson*

NCMEC recognizes that *Wilson* has also affected law enforcement processes. To mitigate *Wilson*'s impact, NCMEC is working on adding a feature for law enforcement which would indicate when a reported file's hash match is the same as that of a file from a previous CyberTipline report. That way, if the "File Viewed by Company" box is not checked (meaning NCMEC cannot view the file), but the file is a hash match to a file NCMEC had viewed in the past (i.e., pre-*Wilson*), law enforcement could go view the file attached to the previous report, rather than get a warrant to view the file attached to the new report. NCMEC told us that the ICAC Task Forces generally support this planned feature.[256] Our understanding is that the completion of this feature is contingent upon the completion of NCMEC's file review process (discussed in Section 6.1), which is expected to take several more years.

[253] Interview with NCMEC staff on December 14, 2023.
[254] Interview with NCMEC staff on November 2, 2023.
[255] Interview with a federal civil servant on October 24, 2023.
[256] Interviews with NCMEC staff between January 30 and February 1, 2024.

7 Findings: Law enforcement agencies

Key findings

- Law enforcement agencies, including ICAC Task Forces and local police departments, are overwhelmed by the volume of actionable CyberTipline reports.
- Law enforcement officers find it challenging to triage accurately, as seemingly low priority reports can lead to the discovery of hands-on abuse.
- There is uncertainty about the necessity of search warrants to view files and needing a search warrant to view files impedes triage, though we did not hear of any search warrant applications to view files being denied.
- While platform employees are divided about whether it is desirable for them to articulate their "hunches" in reports, overworked law enforcement desire such information.
- Frustration arises among law enforcement when platforms fail to accurately complete report fields, and more generally with the prevalence of low-quality reports.
- The practice among some platforms of retaining content for only the legally required 90-day minimum period impedes law enforcement investigations.
- Many law enforcement officers do not focus on internet crimes against children for a long period of time, presenting both benefits and challenges.
- A notable portion of the reports involves victims in the U.S. and offenders located abroad, such as in West Africa.
- Non-U.S. law enforcement agencies encounter additional obstacles, including greater difficulty in obtaining further data from platforms, more stringent privacy regulations that hinder the linking of IP addresses to individuals, capacity constraints, and the challenge of translating reports written in English.

7.1 Report volume

Almost across the board law enforcement expressed stress over their inability to fully investigate all CyberTipline reports due to constraints in time and resources. An ICAC Task Force officer said "You have a stack [of CyberTipline reports] on your desk and you have to be ok with not getting to it all today. There is a kid in there, it's really quite horrible."[257] A single Task Force detective focused on internet crimes against children may be personally responsible for 2,000 CyberTipline reports each year. That detective is responsible for working through all of their tips and either sending them out to affiliates or investigating them personally. This process involves reading the tip, assessing whether a crime was committed, and determining jurisdiction; just determining jurisdiction might necessitate

[257] Interview on August 25, 2023.

multiple subpoenas.[258] Some reports are sent out to affiliates and some are fully investigated by detectives at the Task Force.

An officer at a Task Force with a relatively high CyberTipline report arrest rate said "we are stretched incredibly thin like everyone."[259] An officer in a local police department said they were personally responsible for 240 reports a year, and that all of them were actionable. When asked if they felt overwhelmed by this volume, they said yes. While some tips involve self-generated content requiring only outreach to the child, many necessitate numerous search warrants.[260] Another officer, operating in a city with a population of 100,000, reported receiving 18–50 CyberTipline reports annually, actively investigating around 12 at any given time. "You have to manage that between other egregious crimes like homicides,"[261] they said. This report will not extensively cover the issue of volume and law enforcement capacity, as this challenge is already well-documented and detailed in the 2021 U.S. Department of Homeland Security commissioned report,[262] in Cullen et al.,[263] and in a 2020 Government Accountability Office report.[264] "People think this is a one-in-a-million thing," a Task Force officer said. "What they don't know is that this is a crime of secrecy, and could be happening at four of your neighbors' houses."[265]

We asked a Task Force officer if having more detectives would help with the report volume issue. They expressed uncertainty about this being the sole solution: "I could have ten of me, but I need a team of people who could help me execute search warrants, interview everyone, forensically process [devices], I need people to help with all that. That is now a 6 month process [plus] identifying victims. Then throw in all the reports, trials. It's a lot of work for just one tip."[266] A 2023 Department of Justice strategy report similarly highlighted the delay in child sexual exploitation investigations caused by limited forensic resources.[267]

We spoke with one respondent who previously served in law enforcement and now works at a platform, a background we frequently encountered during our interviews. "We try to respond to law enforcement in the way we wanted platforms to respond when we were in law enforcement," they said, which was also a commonly heard sentiment. They said when they were in law enforcement

[258] Interview with a law enforcement officer on October 12, 2023.
[259] Interview on December 4, 2023.
[260] Interview with a law enforcement officer on December 15, 2023.
[261] Interview on August 7, 2023.
[262] "Supporting Law Enforcement Investigations to Combat Internet Crimes against Children."
[263] Olivia Cullen et al., "'Our Laws Have Not Caught up with the Technology': Understanding Challenges and Facilitators in Investigating and Prosecuting Child Sexual Abuse Materials in the United States," *Laws* 9, no. 4 (2020), https://doi.org/10.3390/laws9040028.
[264] *Online Exploitation of Children: Department of Justice Leadership and Updated National Strategy Needed to Address Challenges,* technical report (United States Government Accountability Office, December 2022), https://www.gao.gov/assets/d23105260.pdf.
[265] Interview on August 18, 2023.
[266] Interview on August 18, 2023. A platform employee who previously worked in law enforcement similarly said: "If you gave me ten times the number of [...] detectives I could have kept them all busy" (date of interview omitted to ensure respondent anonymity).
[267] *National Strategy for Child Exploitation Prevention & Interdiction* (United States Department of Justice, 2023), https://www.justice.gov/d9/2023-06/2023_national_strategy_for_child_exploitation_prevention_interdiction_-_a_report_to_congress.pdf.

they might have 15 active, solid cases they were pursuing. As an example, they described a scenario where a CyberTipline report was received but could not be prioritized due to more urgent cases. By the time they could address the CyberTipline report, the data preservation period had often expired, and the platform would have already discarded crucial account information. Now in industry, the respondent can assess an image and recognize that it is unlikely to be prosecuted based on their law enforcement background, yet they are still required to send it to NCMEC.[268] Still, many respondents said that in an ideal world a report with one known image should still be investigated in case it can lead to uncovering and stopping hands-on abuse.[269]

7.2 Report triage

Given the large volume of reports, law enforcement agencies must triage and prioritize incoming tips. This is an imperfect process (further complicated by the search warrant issue); seemingly innocuous reports have led to high level arrests and high priority tips may lead nowhere in investigations.[270] We spoke with one NGO employee who had formerly worked in law enforcement when report volumes were lower. They recalled regularly investigating CyberTipline reports involving single image uploads. They had the time to identify sophisticated offenders who "slipped up and got one CyberTip." Many of these single image upload tips are not being investigated today due to volume.[271] CyberTipline reports range from "bike theft to intelligence gold" one respondent told us,[272] but it is not always possible to tell which will be which. For example, an investigation triggered by a report about a single image upload led to five arrests, including a perpetrator selling his own son for abuse.[273] One officer told us that they get many big cases out of single file reports that have received the lowest priority rating.[274]

Law enforcement pick a certain percentage of reports to investigate. The selection is not done in a very scientific way—one respondent described it as "They hold their finger up in the air to feel the wind."[275] An ICAC Task Force officer said triage is more of an art than a science. They said that with experience you get a feel for whether a case will have legs, but that you can never be certain, and yet you still have to prioritize something.[276]

Many respondents mentioned they prioritize reports containing names familiar to them, such as registered sex offenders or prominent community members in

[268] Interview on October 20, 2023.
[269] Interview with a lobbyist on October 20, 2023.
[270] Interview with a federal department employee on November 2, 2023.
[271] Interview with an NGO employee on October 10, 2023.
[272] Interview on August 15, 2023 with an employee of a company that creates software for law enforcement.
[273] The AviaTor Project, "Save Time, Save Lives."
[274] Interview with a law enforcement officer on January 4, 2024.
[275] Interview with an NGO employee on July 31, 2023.
[276] Interview on August 25, 2023.

positions of trust—like a firefighter or a teacher.[277] However, this is not always feasible, as not all CyberTipline reports include real names. One respondent mentioned that those who are not known to law enforcement present an unknown risk, and should perhaps be prioritized even over known sex offenders.[278] Integration with other APIs, such as the peer-to-peer file-sharing API discussed in Section 6.2, could assist in prioritizing among unknown individuals. Another respondent said that while in law enforcement they prioritized reports from a platform where assessing culpability was straightforward due to the nature of the platform.[279]

There is a whole industry of companies globally that exist to help law enforcement enrich CyberTipline reports. These companies fill a gap by comparing new tips with old tips, doing fuzzy matching, comparing avatars, and creating similarity rankings.[280] This report enrichment helps law enforcement better triage tips. Even if NCMEC were better able to enrich tips at scale, it is likely that this industry would still exist, as there is enrichment that can happen based on internal police databases.

7.3 Perspectives on reports unlikely to lead to prosecution

There are some CyberTipline reports that many agree should not be prosecuted, such as outrage shares and memes. But without platforms more consistently leveraging relevant CyberTipline checkboxes, it is not clear what more about the current system should be changed to solve that issue. U.S. law requires that platforms report this content if they find it, and that NCMEC send every report to law enforcement.[281] When NCMEC knows a report contains viral content or memes they will label it "informational," a category that U.S. law enforcement typically interpret as meaning the report can be ignored, but not all such reports get labeled "informational." Additionally there are an abundance of "age difficult" reports that are unlikely to lead to prosecution. Law enforcement may have policies requiring some level of investigation or at least processing into all non-informational reports. Consequently, officers often feel inundated with reports unlikely to result in prosecution. In this scenario, neither the platforms, NCMEC, nor law enforcement agencies feel comfortable explicitly ignoring certain types of reports. An employee from a platform that is relatively new to NCMEC reporting expressed the belief that "It's best to over-report, that's what we think." They then asked us, "Is that right?"[282]

An officer expressed frustration over platforms submitting CyberTipline reports that, in their view, obviously involve adults: "Tech companies have the ability to [...] determine with a high level of certainty if it's an adult, and they need to

[277] Interview with a law enforcement officer on August 18, 2023.
[278] Interview with an NGO employee on July 31, 2023.
[279] Interview with a platform employee who previously worked in law enforcement. Date omitted to ensure respondent anonymity.
[280] Interview with a company that contracts with law enforcement on October 18, 2023.
[281] 18 U.S.C. § 2258A(c). If NCMEC cannot assess jurisdiction they make the report available to federal U.S. law enforcement.
[282] Interview on November 15, 2023.

stop sending [tips of adults]."[283] This respondent also expressed a desire that NCMEC do more filtering in this regard. While NCMEC could probably do this to some extent, they are again limited by the fact that they cannot view an image if the platform did not check the "reviewed" box (Figure 5.3 on page 26). NCMEC's inability to use cloud services also makes it difficult for them to use machine learning age classifiers. When we asked NCMEC about the hurdles they face, they raised the "firehose of I'll just report everything" problem.[284]

A former employee of a platform that sends many CyberTipline reports said, "People who are in the trenches kind of roll their eyes at this harsh rule that you have to report everything when you just know it's a viral meme. It's 30 years old. Law enforcement will never investigate this. [...] But it's hard politically to argue that some stuff shouldn't be reported. It's almost a religious fight that takes on almost religious tones."[285] They added that while it might be politically untenable to flag a report as being less important (though of course platforms are encouraged to flag reports if they contain memes), many platforms think about ways they can signal that a tip is more important. This is likely helpful, but does not address the issue that law enforcement may still have to spend time processing all non-informational CyberTipline reports.

CyberTipline reports also include instances where the offender operates from outside the U.S. A recent trend involves U.S. children being targeted by sextortion schemes orchestrated by offenders in West Africa for monetary gain.[286] Although U.S. law enforcement has made some efforts to collaborate with international counterparts to prosecute these offenders,[287] these reports often do not result in arrests. Law enforcement officials also find certain types of reports particularly challenging, especially those that do not depict activities considered illegal in specific jurisdictions. For example, grooming is not uniformly defined or criminalized across the U.S., adding to the complexity and frustration of handling these tips. In Arizona, for instance, the state legislature introduced a bill to define and criminalize grooming in January 2024, but as of writing it has not yet been voted on in the state senate.[288]

7.4 Reports and hunches

One law enforcement officer provided an interesting example of a type of report he found frustrating: he said he frequently gets reports from one platform where

[283] Interview with a law enforcement officer on October 12, 2023.

[284] Interview on November 2, 2023.

[285] Interview on September 22, 2023.

[286] "FBI and Partners Issue National Public Safety Alert on Financial Sextortion Schemes," United States Attorney's Office, Western District of Washington, December 19, 2022, https://www.justice.gov/usao-wdwa/pr/fbi-and-partners-issue-national-public-safety-alert-financial-sextortion-schemes.

[287] "Three Nigerian Men Awaiting Extradition For Committing Sexual Extortion," United States Attorney's Office, Western District of Michigan, May 3, 2023, https://www.justice.gov/usao-wdmi/pr/2023_0503_Sextortion_Indictment.

[288] Caitlin Sievers, "Bill to criminalize 'grooming' children moves forward," *Arizona Mirror*, January 24, 2024, https://azmirror.com/2024/01/24/bill-to-criminalize-grooming-children-moves-forward/.

an account was hacked and then used to share CSAM. This platform provided the dates of multiple password changes in the report, which the officer interpreted as indicating the account had been hacked. Despite this, they felt obligated to investigate the original account holder. In a recent incident they described, they were correct that the account had been hacked. They expressed that if the platform explicitly stated their suspicion in the narrative section of the report, such as by saying something like "we think this account may have been hacked," they would then feel comfortable de-prioritizing these tips.[289] We subsequently learned from another respondent that this platform provides time stamps for password changes for all of their reports, putting the burden on law enforcement to assess whether the password changes were of normal frequency, or whether they reflected suspicious activity.

With that said, the officer raised a valid issue: whether platforms should include their interpretation of the information they are reporting. One platform employee we interviewed who had previously worked in law enforcement acknowledged that they would have found the platform's unwillingness to explicitly state their hunch frustrating as well.[290] However, in their current role they also would not have been comfortable sharing a hunch in a tip: "I have preached to the team that anything they report to NCMEC, including contextual information, needs to be 100% accurate and devoid of personal interpretation as much as possible, in part because it may be quoted in legal process and case reports down the line." They said if a platform states one thing in a tip, but law enforcement discovers that is not the case, that could make it more difficult for law enforcement to prosecute, and could even ruin their case. Relatedly, a former platform employee said some platforms believe if they provide detailed information in their reports courts may find the reports inadmissible.[291] Another platform employee said they avoid sharing such hunches for fear of it creating "some degree of liability [even if] not legal liability" if they get it wrong.[292]

The platform employee who is against sharing hunches noted one exception to this policy: sex trafficking. CyberTipline reports for sex trafficking can be "highly subjective," and in these tips they will use "caveat language." They believe the risk of not reporting sex trafficking, even if it demands interpretation, is "far greater than the risk of possibly providing misinterpreted information." The comparative lack of clarity in sex trafficking indicators is reflected in proposed federal legislation. In requiring platforms to start reporting apparent child sex trafficking, the legislation would also permit NCMEC to release guidelines for platforms about how to identify it.[293]

As is evident, there is variation in opinion among platforms about whether sharing such investigative hunches is appropriate. We were able to see reports from a platform that is known for providing extensive supplemental documentation for their high priority reports.[294] Law enforcement find these reports exceptionally

[289] Interview with a law enforcement officer on December 15, 2023.
[290] Interview by email on January 18, 2024.
[291] Interview with a former platform employee on December 20, 2023.
[292] Interview with a platform employee on March 6, 2024.
[293] REPORT Act.
[294] This platform did not show us their reports. We viewed them via a different respondent.

helpful. The platform appears to balance the importance of caution with the fact that they are best placed to investigate activity on their own platform by repeatedly using language suggesting that their assessments should be verified. This appears to us to be a useful middle ground: trust but verify. One platform told us they are comfortable providing hunches because "we are not a prosecutor trying to prove something beyond a reasonable doubt [...] we are not a judge or jury."[295]

7.5 Report reliability and actionability

The phrase "unactionable tip" came up frequently in law enforcement interviews. Some reports seem genuinely unactionable, such as a report originating from a platform that offers user anonymity and only provides a ten-year-old registration IP address, leaving little to no scope for follow-up action.[296] One officer at a local police department reports that 90% of the reports they receive are "garbage;" this is striking, as they are only receiving tips that their Task Force chose to send on to him, and hints at the high portion of reports law enforcement do not find useful.[297] In contrast, a law enforcement officer in a well-resourced police department argued that very few CyberTipline reports that they receives from his Task Force are truly unactionable.[298] To some extent, whether a report is actionable depends on available resources.

Another area of frustration for law enforcement was platforms' inconsistency in completing the CyberTipline reporting form. They complain about platforms not using the report fields correctly. "Providers have been told hundreds of times by law enforcement how to fill out the report," one respondent told us,[299] perceiving that issues in completing fields are due to the platform not investing sufficient engineering time into their tip filing process. Potentially related, there are complaints about platforms providing insufficient information in the tips. The more information that is provided, the easier it is for the Task Forces to, for example, assess jurisdiction of the tip without having to ask a platform for additional information.[300]

Inconsistent platform behavior can make investigators reluctant to rely on platforms' representations in their reports. One employee of a federal department said that to minimize the risk of suppression by a court, some federal government employees will seek a search warrant before viewing a file even if the platform checked the "File Viewed by Company" box, out of concern that some platforms check the "Filed Viewed by Company" box if the image *has ever* been reviewed, even if it was not reviewed in this particular case.[301]

[295] Interview on February 8, 2024.
[296] Interview with a law enforcement officer on August 18, 2023.
[297] Interview with a law enforcement officer on December 15, 2023.
[298] Interview with a law enforcement officer on September 18, 2023.
[299] Interview on August 15, 2023 with an employee of a company that makes software for law enforcement.
[300] Interview with a a law enforcement officer on October 12, 2023.
[301] Interview on November 2, 2023.

We heard both praise and criticism from law enforcement about virtually all of the large platforms' reporting practices. The platforms that report the most are likely doing the most scanning for CSAM, but at that volume the raw number of CyberTipline reports not supplemented by a manual investigation or viewed by the platform will be highest.

Law enforcement complain about platforms being trigger happy when it comes to prioritization. Both platforms and NCMEC have the ability to escalate a report. Law enforcement complain that some platforms label CyberTipline reports as high priority when they contain messaging indicative of someone being sextorted. Multiple law enforcement officers said that when they see a CyberTip that is labeled high priority they drop everything to respond. In these cases, however, the offender is often in a different jurisdiction, commonly in West Africa. And while it is important to identify the victim and their family and provide resources—sextortion can escalate to self harm or suicide[302]—law enforcement do not feel these tips justify a priority label.[303] Rightly or wrongly, they perceive that platforms are escalating these to shift the blame to law enforcement if anything happens to the victim. "There's a lot of bad blood" between law enforcement and platforms, one respondent said, referring to the tension at some roundtables NCMEC holds for both. He added that it is intimidating for platform employees to walk into a room full of angry law enforcement officers.[304]

We heard frustration from many types of respondents, including law enforcement officers, about the perceived quality of various hash datasets.[305] The respondents felt that a hash match against some datasets may not indicate CSAM. One respondent told us that judges are aware of the imperfections of the hash databases and will tend to be more understanding toward prosecutors if they present hash matches to numerous databases as opposed to just one or two.[306] There have been cases, however, where platforms complain about the quality of a single hash, but when NCMEC looks at images they know that even though it appears to be an adult, they had previously identified the individual as a child.[307]

7.6 Reactive versus proactive investigations

ICAC Task Forces have varying policies about reactive work—like investigating CyberTipline reports—versus proactive work, such as complex investigations of ongoing crimes. Law enforcement officers disagree on this topic as well. One officer said they prefer to prioritize CyberTipline reports, and are satisfied with

[302] Ken Dilanian, "Nigeria hands over two suspects in sextortion case linked to suicide of Michigan high school athlete," *NBC News*, August 14, 2023, https://www.nbcnews.com/politics/justice-department/us-extradites-nigerians-sextortion-linked-suicide-michigan-teen-rcna99795.

[303] Interview with a law enforcement officer on August 25, 2023.

[304] Interview with an employee of a company that provides services to law enforcement on October 18, 2023.

[305] For an example of a hash dataset audit, see: Patricia Davis, "Helping Child Survivors: The Fight to Remove Sex Abuse Images," April 15, 2024, https://www.missingkids.org/blog/2024/helping-child-survivors-fight-to-remove-sex-abuse-images.

[306] Interview with a law enforcement officer on September 18, 2023.

[307] Interview with NCMEC staff on November 13, 2023.

the ratio of reports that are leading to a child being rescued.[308] Others argue that prioritizing undercover investigations is more important because these investigations result in intercepting adults before abuse happens.[309] One law enforcement officer described undercover proactive work as "shooting fish in a barrel. You put up an account and immediately people start reaching out." While some of their colleagues believe that proactive work should be prioritized over CyberTipline report investigations, they do not feel like one is more or less valuable than the other, noting that seemingly straightforward "upload/download" tips often lead to the discovery of hands-on abuse.[310]

7.7 Search warrants and preservation requests

If law enforcement decide to fully investigate a tip, they will usually request a search warrant to compel the platform to provide additional account information. Law enforcement respondents say that some platforms have a reputation for being difficult to get this information from. The platform may be slow to respond and may provide information in a hard-to-access format. Both issues can lead to delays in prosecution, which can cause issues with judges. Law enforcement may have the option to issue a non-disclosure order, telling the platform not to inform the user about the search warrant, but there are known instances where platforms fail to comply with those orders. In some cases, law enforcement will request account-level information, only to discover that the platform did not preserve information beyond the minimum 90 day preservation period. We heard about one platform whose practice was to delete all account information except the reported content after a report was made,[311] though another platform told us it preserves everything about the account and the reported content.[312]

One former platform employee mentioned that the law is unclear about the preservation requirements for platforms.[313] The law requires preservation of the contents provided in the CyberTipline report, but above and beyond that, states only that "a provider shall preserve any visual depictions, data, or other digital files that are reasonably accessible and may provide context or additional information about the reported material or person."[314] This ambiguity gives platforms leeway in choosing how much or how little to preserve. Spelling out specifics in the statute would be challenging given the broad variety in online products and services and in the types of data that different platforms collect. Law enforcement may find it frustrating when a platform has not preserved data, but that is a result of the statute's lack of clarity.[315]

[308] Interview on December 15, 2023.
[309] Interview with a law enforcement officer on August 25, 2023.
[310] Interview with a law enforcement officer on September 18, 2023.
[311] Interview with a law enforcement officer on September 18, 2023.
[312] Interview with a platform employee on November 6, 2023.
[313] Interview on October 6, 2023.
[314] 18 U.S.C. § 2258A(h)
[315] Interview on October 6, 2023.

While some platforms preserve data for 180 days, many platforms only preserve data for the required minimum of 90 days. This can impede investigations. NCMEC's initial review and triage of a report can take hours to days. NCMEC then sends it to a Task Force where it enters their queue before being reviewed and forwarded to a local Task Force affiliate. The local officer must then review the report and submit for a search warrant. By the time the local officer has received the warrant, 90 days may have passed and the platform may have no retained information to provide.[316] Members of law enforcement report that more tips would be actionable if platforms were required to retain content for longer.[317] Extending the preservation period has been proposed in multiple pending U.S. child safety bills.

In addition to data retention issues, law enforcement officers need to know what information to include in their search warrants. Law enforcement express frustration that platforms frequently change the way their data is structured, and may not keep information about what data is available via search warrants up to date.[318] There are many consequences if a platform provides data in an unmanageable format. One assistant district attorney said that "if someone comes in and says they will plead to [some crime], and the data [that police received from a platform] is impossible to go through, prosecutors are more likely to take a plea."[319] Not all respondents felt the same way. Referring to the same platform, which is notorious for providing data in a difficult to access format, the officer in a well-resourced police department said: "It's not that dire. We would never not investigate a case because of the behavior of [a platform]." That officer had a whole team of people who could restructure the data into an accessible format.[320]

In our interviews, law enforcement also conveyed the professional hurdles to developing CyberTipline expertise. Many people who start working at ICAC Task Forces find that the work is too intense and need to leave.[321] A civil servant in the federal government told us that they had an employee say they could not continue the work anymore, and went on to focus on human trafficking, which they felt to be less intense. "[You need to] respect that," the civil servant said. "There are people who stay and people who go."[322] If you are a local police officer and want to progress your career in law enforcement, it is important to be well-rounded and not pigeon-holed into one area. Police may work on sexual exploitation issues for a year, and then be rotated, limiting the ability for expert knowledge accumulation. There are advantages to this approach—one being that dealing with this topic for too long can have wellness implications for some people. Investigating CSAM is unique, one respondent said. "It's not like officers have to take the fentanyl to

[316] Interview with a law enforcement officer on September 18, 2023.
[317] Interview with a law enforcement officer on December 15, 2023.
[318] Interview with a law enforcement officer on August 18, 2023.
[319] Interview on August 17, 2023.
[320] Interview with a law enforcement officer on September 18, 2023.
[321] See Cullen et al., "'Our Laws Have Not Caught up with the Technology': Understanding Challenges and Facilitators in Investigating and Prosecuting Child Sexual Abuse Materials in the United States" for a summary of research on the wellness implications of viewing CSAM for law enforcement. *Online Exploitation of Children* (*Online Exploitation of Children*) also discussed challenges related to retaining skilled workers.
[322] Interview with a federal civil servant on October 24, 2023.

testify about it."[323]

At the same time, informal knowledge about the process for investigating CyberTipline reports is not formalized in many departments. A platform employee who used to work in law enforcement said that investigators new to CyberTipline reports may not understand the importance of submitting preservation requests to platforms as soon as possible. They may also reach out informally to the platform for information to bolster their search warrant, but the platforms generally are not legally allowed to respond to these inquiries.[324] Experienced law enforcement officers describe a temptation among detectives newer to this work to stop investigating once they get enough evidence for a lesser charge of CSAM viewing or distribution. Experienced officers emphasized the importance of continuing the investigation until you can rule out hands-on abuse.

CSAM cases also require specialized forensic investigation skills. To charge a perpetrator prosecutors need to place the user at a device at a particular time to prove beyond a reasonable doubt that another person had not had access to the device at the time of the crime. Not all forensic specialists understand the specific information needed to prosecute cases involving the online sexual exploitation of a child.

7.8 Local law enforcement prioritization of crimes against children

There is a related challenge that ICAC Task Forces face: affiliates. These are law enforcement agencies with detectives who have been trained by Task Forces to investigate internet crimes against children, including CyberTipline reports. Some Task Forces have many affiliates, and can thus send many of their CyberTipline reports to local law enforcement. Other Task Forces have fewer affiliates, and therefore must investigate more of the tips in-house.

A former Task Force officer described the barriers to training more local Task Force affiliates. In some cases local law enforcement perceive that becoming a Task Force affiliate is expensive, but in fact the training is free.[325] In other cases local law enforcement are hesitant to become a Task Force affiliate because they will be sent CyberTipline reports to investigate, and they may already feel like they have enough on their plate. Still other Task Force affiliates may choose to unaffiliate, perceiving that the CyberTipline reports they were previously investigating will still get investigated at the Task Force, which further burdens the Task Force. Unaffiliating may also reduce fear of liability for failing to promptly investigate a report that would have led to the discovery of a child actively being abused,[326] but the alternative is that the report may never be investigated at all.

[323] Interview with a former platform employee on October 6, 2023.
[324] Interview with a platform employee on October 20, 2023.
[325] Interview on September 22, 2023.
[326] Interview with a law enforcement officer on October 12, 2023.

While there are cases of local law enforcement agencies unaffiliating, since 2016 the total number of affiliates has increased.[327]

This liability fear stems from a case where six months lapsed between the regional Task Force receiving NCMEC's report and the city's police department arresting a suspect (the abused children's foster parent). In the interim, neither of the law enforcement agencies notified child protective services about the abuse as required by state law. The resulting lawsuit against the two police departments and the state was settled for $10.5 million.[328] Rather than face expensive liability for failing to prioritize CyberTipline reports ahead of all other open cases, even homicide or missing children, the agency might instead opt to unaffiliate from the ICAC Task Force.[329] One officer who was familiar with this unaffiliating phenomenon in nearby small towns described this behavior as egregious: "How can you do that? That's like someone from the public coming in to report their car was stolen and you say yeah sorry we're not going to do [anything about] that. How can you do that with a child and not dedicate [some resources] to that?"[330]

Many law enforcement respondents said they felt like their chiefs did not understand the importance of CyberTipline reports. One respondent said they perceived that their higher ups did not read their descriptions of child exploitation, not wanting to be exposed to it.[331] Another respondent said that higher ups would "wince at my descriptions, but they still wouldn't prioritize our cases."[332] Many respondents brought up burglaries, perceiving that CyberTipline reports are more important to investigate than burglaries, but that there can be pressure to investigate burglaries in part related to insurance claims.[333] One respondent observed a mismatch between how much U.S. society prioritizes crimes against children and the resources officers who focus on this crime receive.[334] Law enforcement officers additionally mentioned the importance of ensuring prosecutors understood the crime. Very detailed written descriptions of media can be useful for this.

7.9 Perspectives from prosecutors and defense attorneys

It is not just police chiefs who may shy away from CSAM cases. An assistant U.S. attorney said that potential jurors will disqualify themselves from jury duty to avoid having to think about and potentially view CSAM. As a result, it can take longer than normal to find a sufficient number of jurors, deterring prosecutors

[327] Interview on March 7, 2024.

[328] Jack Connelly and Lincoln Beauregard, *Albertson v. State of Washington DSHS*, 2008, https://www.connelly-law.com/results/civil-rights-results/albertson-v-state-of-washington-dshs/; John Iwasaki, "Seattle settles in foster kids' suit," *Seattle Post-Intelligencer*, July 9, 2008, https://www.seattlepi.com/seattlenews/article/seattle-settles-in-foster-kids-suit-1278824.php.

[329] Interview with a law enforcement officer on October 12, 2023.

[330] Interview with a law enforcement officer on December 15, 2023.

[331] Interview with a law enforcement officer on September 18, 2023.

[332] Interview with a law enforcement officer on October 12, 2023.

[333] Interview with a law enforcement officer on September 18, 2023.

[334] Interview with a platform employee who previously worked in law enforcement. Date of interview omitted to ensure respondent anonymity.

from taking such cases to trial.[335] There is a tricky balance to strike in how much content to show jurors, but viewing content may be necessary. While there are many tools to mitigate the effect of viewing CSAM for law enforcement and platform moderators, in this case the goal is to ensure that those viewing the content understand the horror. The assistant U.S. attorney said that they receive victim consent before showing the content in the context of a trial. Judges may also not want to view content, and may not need to if the content is not contested, but seeing it can be important as it may shape sentencing decisions.

Having juries view CSAM can also be important for overcoming what one assistant district attorney called the "victimless mindset." For many cases, they added, "we don't have the kids that can come in [a courtroom] and do the pulling on the heart strings."[336]

Our interviews with prosecutors were interesting in that the CyberTipline report is often not that relevant to them. The report starts the investigation, but by the time the prosecutor is looking at the evidence the CyberTipline report has become mostly irrelevant. It was simply, as the name suggests, a tip. However, from the defense perspective, everything stemmed from the tip. If the tip can be dismissed, the whole case can be dismissed. That said, a defense attorney noted that judges will try hard to not throw out a CyberTipline report.[337]

One defense attorney told us that CyberTipline reports are an imperfect way to identify suspects. A username and an email in a report is simply information the platform observed—it should not mean that the person who owns the email is a suspect. Platforms may not require email verification, so in some cases a user could register for an account with an email they don't own.[338]

Defense attorneys report issues with prosecutors incorrectly claiming images or videos are of children, when in fact they show adults. A former assistant federal public defender told us a story about how they once had a colleague view a video that their client was being charged with possessing. They wanted their colleague to confirm the video was CSAM. "I didn't feel comfortable pleading someone without (at least someone) looking." The colleague informed them that the video was an adult pornography star who did "age play stuff."[339] The case was dismissed. It is for this reason, the respondent told us, that prosecutors tend to charge on known content, so they don't have to do investigative work to prove that the media is CSAM. "Even if the client has 500 videos," they said, "they'll charge the 16 that are known content."[340] One defense attorney brought up a well-known case from 2010 when an adult pornography actress appeared in court on behalf of a defendant charged with transporting CSAM to prove that

[335] Interview with an assistant district attorney on August 17, 2023; Interview with an assistant U.S. attorney on August 28, 2023.

[336] Interview on August 17, 2023.

[337] Interview on August 18, 2023.

[338] Interview with an assistant federal public defender on August, 18, 2023.

[339] It is an affirmative defense to CSAM receipt and possession offenses that the alleged CSAM depicts someone who was an adult at the time it was produced. 18 U.S.C. § 2252A, https://www.law.cornell.edu/uscode/text/18/2252A(c).

[340] Interview on August 24, 2023.

she was an adult.[341] Another assistant federal public defender told us that Sexual Assault Nurse Examiners (SANE) who prosecutors ask to testify as to the age of an individual in media will say anyone is under the age of 18: "Their SANE nurse would say my grandmother was under 18."[342] (We note that prosecutors generally speak very highly of SANE nurses.)

There is a sense among defense attorneys that jurors are biased against their clients; a defense attorney interviewed a juror after a case and got the sense that the juror did not understand that the government had the burden of proving guilt.[343]

While we did not interview many prosecutors, we have the sense that prosecutors are not drowning in child sexual exploitation cases.[344] Law enforcement are bringing them a manageable amount of cases. Both prosecutors and defense attorneys report that most CSAM cases plead out (as is the case with most crimes). "You don't want to be presenting these issues to a jury unless you have a very unusual defense," one assistant federal public defender told us. "[CSAM] possessors are not viewed very sympathetically by juries."[345]

Though beyond the scope of our research, CSAM possession sentencing guidelines came up repeatedly in interviews—both with prosecutors and defense attorneys. Across the board respondents viewed sentences as overly long—and said many (though not all) judges feel the same way. After the 2003 PROTECT Act caused average sentence lengths and recommended sentencing ranges to increase significantly for non-production offenses, judges have responded by frequently giving sentences below the recommended range, and the U.S. Sentencing Commission has recommended reforms to more closely align sentencing to today's technology-enabled offenses.[346] As things stand, "it's not really a system that inspires much confidence," the assistant federal public defender said. "There isn't diversion or treatment, it's just prison."[347] A former assistant federal public defender said: "The core [CSAM] case isn't a producer or someone with a history of contact offenses. The psychosexual background comes back low-risk. A lot of them are veterans and have post-traumatic stress disorder, some have pretty low IQ." They noted that a lot of the "downloader offenders [...] aren't the predators we think of. They have mental issues [...] and start [...] downloading edgier and edgier stuff."[348]

[341] Todd Venezia, "A trial star is porn," *New York Post*, April 24, 2010, https://nypost.com/2010/04/24/a-trial-star-is-porn/.
[342] Interview with an assistant federal public defender on September 14, 2023.
[343] Id.
[344] Interview with an assistant district attorney on August 17, 2023.
[345] Interview on August 18, 2023.
[346] United States Sentencing Commission, Federal Sentencing of Child Pornography: Non-Production Offenses, No. 110-401, June 2021, https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2021/20210629_Non-Production-CP.pdf.
[347] Interview on August 18, 2023.
[348] Interview on August 24, 2023.

7.10 Legal considerations for U.S. law enforcement

7.10.1 Law enforcement and the Fourth Amendment

Fourth Amendment concerns are even more salient for investigators and prosecutors than for NCMEC: they are indisputably government actors and must carefully observe the boundaries of government agency doctrine and private search doctrine or else risk the suppression of evidence in investigations.

When it comes to government agency doctrine (under *Ackerman* and other cases), law enforcement agents realize that they are walking "a fine line" in their interactions with platforms.[349] When communicating with platforms about CyberTipline reporting practices, federal agencies will phrase things broadly rather than ask for specific information. They can say to platforms that while there is not any information they are required to include in a CyberTip, the more information investigators have, the better. They run into roadblocks when a CyberTip does not give them enough information to act.[350] To back that up, they may point to NCMEC's statistics about how many providers' reports consistently lacked adequate, actionable information.[351]

In the context of private search doctrine, *Wilson*, like *Ackerman* before it, held that government actors must get a warrant to open files which the reporting platform had not reviewed.[352] Since NCMEC stopped opening and triaging reports that the platform did not view, it is up to law enforcement to decide which tips to get warrants for (with triage being complicated by the catch-22 of not being able to warrantlessly open the files). Even outside of the *Ackerman* and *Wilson* circuits, federal law enforcement now tends toward a more cautious approach and gets warrants to avoid potentially undermining a case, even if it is fairly certain that the private search doctrine has been satisfied.[353] That means law enforcement will opt for a warrant even if the "File Viewed by Company" box is checked.

Although there is variation in what checking the "File Viewed by Company" box on the CyberTipline report form means, it seems likely that reports where a human looked at the file(s) are at least slightly more likely to be investigated, as there is less friction in beginning the investigation if the reported content arguably does not require a warrant for NCMEC or law enforcement to view. In contrast to risk-averse federal prosecutors, depending on state laws, state-level investigators may be more likely to open files without getting warrants.[354] But in practice, according to one platform employee, if the box is not checked, investigators will not open the file even if the case law in their district might allow it.[355] One officer we interviewed pulled up their internal system for tracking CyberTipline reports

[349] Interview with a federal department employee on December 11, 2023.
[350] Id.
[351] Id; NCMEC, "CyberTipline 2022 Report."
[352] *Wilson*, 13 F.4th at 971–74; *Ackerman*, 831 F.3d at 1305–7.
[353] Interviews with federal department employees on November 2 & 17, 2023.
[354] Eid.
[355] Interview with a platform employee on August 4, 2023.

and eyeballed that about half of the tips had the "File Viewed by Company" box checked.[356]

In an environment where investigators receive a high volume of CyberTipline reports but the meaning of a checkbox on the form can be uncertain, one way law enforcement has implemented the *Wilson*/*Ackerman* warrant requirement is through the practice of so-called "batch warrants." One local officer in a U.S. city shared that their ICAC Task Force applies for batch warrants for all tips where the "File Viewed by Company" box was not checked. "They do these warrants in 'batches' to prevent the judges from having to read hundreds of the same thing," they explained. Each warrant application batches together multiple CyberTipline reports at once, with a probable cause statement asking for permission to view content for all the tips in that batch (which may number in the hundreds), listed by report number. The "batched" CyberTipline reports are not necessarily linked or related; their only commonality is the need for a search warrant.[357] Batch warrants have been used in Ninth Circuit courts (which are bound by *Wilson*) to deal with a high volume of tips from a single platform during a single time period.[358] Batch warrants can be an effective tool; after all, there are tons of CyberTipline reports and only so many judges, and judicial resources are a bottleneck just like prosecutorial and investigative resources. Batch warrants are still time consuming to request and some judges are more willing to grant them than others.[359]

There is no question that getting a warrant slows investigators down or that it takes careful work to prepare a search warrant application and lay out the probable cause, particularly since every platform is unique and so applications cannot be one-size-fits-all. That said, one public defender commented that they would be shocked if a judge turned down a search warrant application that was based solely on a CyberTipline report.[360] And in fact, federal department employees we interviewed admitted that they had never heard of a federal judge rejecting a search warrant application to open attachments to a report—indeed, at least one federal magistrate judge does not think a warrant is needed for CyberTipline reports at all.[361] A law enforcement officer likewise confirmed never having had a CyberTipline report search warrant application rejected.[362] This accords with *Ackerman*'s prediction in 2016 that investigators would have no trouble getting warrants to open report attachments.[363] Still, law enforcement could use more clarity about whether and when they need a warrant. The legal landscape now makes it riskier not to get a warrant lest they undermine their case.[364]

Finally, as one respondent pointed out, *Ackerman* and *Wilson* have a human toll.

[356] Interview on August 18, 2023.

[357] Interview with a law enforcement officer on September 18, 2023.

[358] Interview with federal department employees on December 11, 2023.

[359] Interviews with federal department employees on November 17 and December 11, 2023.

[360] Interview with an assistant federal public defender on August 18, 2023.

[361] Interview with federal department employees on December 11, 2023.

[362] Interview with a law enforcement officer on December 15, 2023 (noting having only done a couple such warrants).

[363] *Ackerman*, 831 F.3d at 1309 ("[W]e are confident that NCMEC's law enforcement partners will struggle not at all to obtain warrants to open emails when the facts in hand suggest, as they surely did here, that a crime against a child has taken place.").

[364] Interview with federal department employees on December 11, 2023.

To the extent it has caused platforms to do more human review when submitting CyberTipline reports, the *Wilson* view of the Fourth Amendment private search doctrine effectively requires traumatizing platform workers. That burden should not fall on them, the respondent said; in general the unavoidable trauma of viewing CSAM should fall to those tasked with enforcing the laws against it.[365]

7.10.2 Statutory restrictions

Investigators are mindful not just of Fourth Amendment considerations, but also statutory restrictions governing platforms' disclosure of user data. The federal Stored Communications Act (SCA) distinguishes between permissible voluntary disclosures of user data by platforms (which do not require legal process) and compelled disclosures (which do).[366] While initial reports to NCMEC are classed as voluntary,[367] legal process is needed for investigators' follow-up on those reports. The type of information being sought dictates the required form of process. The SCA requires a warrant from a judge for the contents of files and emails, whereas basic information about an account can be obtained with just a government-issued administrative subpoena.[368] State laws also vary in terms of what type of legal process is required for what information.

Investigators can get an account holder's name, email, IP address, and physical address with a subpoena,[369] but getting additional information may require additional process such as a search warrant, adding more steps to the investigation.[370] Just determining which law enforcement agency has jurisdiction over a particular report may require multiple subpoenas to multiple entities (such as ISPs).[371] Most platforms are willing to work with law enforcement, but some pride themselves on not being law enforcement-friendly.[372]

In short, the legal landscape for investigators to obtain user data is in a constant state of dynamic change. Both courts and platforms continually evolve their interpretations of privacy laws, platforms continually make changes to what data they collect and how long they retain it, and given how many platforms there are, it can be hard for investigators to keep up.[373]

[365] Interview with a former criminal defense lawyer on October 4, 2023.
[366] Interview with federal department employees on December 11, 2023; see also 18 U.S.C. § 2702, https://www.law.cornell.edu/uscode/text/18/2702 (voluntary disclosures under the SCA), 18 U.S.C. § 2703, https://www.law.cornell.edu/uscode/text/18/2703 (required disclosures pursuant to legal process).
[367] 18 U.S.C. § 2702(b)(6), (c)(5).
[368] 18 U.S.C. § 2703. The need for a warrant ultimately comes from the Fourth Amendment, not the SCA. United States v. Warshak, 631 F.3d 266 (6th Cir. 2010), https://perma.cc/W9DW-YTC7.
[369] Interview with assistant federal public defender on August 18, 2023; Interview with a law enforcement officer on August 18, 2023; see also 18 U.S.C. § 2703(c)(2).
[370] Interview with an Assistant U.S. Attorney on August 28, 2023.
[371] Interview with a law enforcement officer on October 12, 2023.
[372] Id.
[373] Interview with a law enforcement officer on August 18, 2023.

7.11 The CyberTipline and non-U.S. law enforcement

7.11.1 Data challenges outside the U.S.

While this paper has focused on CyberTipline challenges in the U.S., challenges outside the U.S. are even greater. U.S. federal law authorizes (but does not require) NCMEC to send reports to non-U.S. law enforcement. NCMEC generally focuses its efforts on the U.S. and automatically sends reports abroad based on geographic indicators, except in cases where NCMEC escalates a report or a country is paying for a dedicated NCMEC analyst.[374] For countries with limited law enforcement capacity, the influx of CyberTipline reports—which, like in the U.S., will include a mix of urgent tips where a child needs to be rescued alongside a huge portion of memes—can be overwhelming. “The tap is turned on and the handle has been removed,” one NGO employee said, describing the CyberTipline situation in an African country.[375]

While law enforcement in the U.S. may complain about the process of getting additional account information from platforms, they at least have the ability to request a search warrant. This is of course not an option for non-U.S. law enforcement. To obtain evidence from a U.S.-based platform, foreign law enforcement generally must follow the procedures required by the mutual legal assistance (MLA) treaty between that country and the U.S. Foreign law enforcement agencies commonly send and receive MLA requests in CSAM investigations.[376] But the MLA process is considered slow and inefficient,[377] taking about 10 months according to one 2013 estimate[378] and 12–24 months according to one respondent.[379] A 2018 U.S. law lets qualified countries enter an agreement with the U.S. to bypass MLA and serve electronic evidence demands directly on U.S. providers, but so far only the U.K. and Australia have done so.[380] Most foreign law enforcement thus still face MLA delays.

Even if the initial report had sufficient information to start an investigation, if there was a delay in the offending content reaching the appropriate law enforcement officer—a delay that could be due to the platform, NCMEC, or foreign law enforcement—it may be difficult to investigate. Even in the U.S., law

[374] Interview with an NGO employee on November 6, 2023.

[375] Interview on December 5, 2023.

[376] T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, Dec. 2014, https://rm.coe.int/16802e726c.

[377] *Id.* at 3. (“In practice, however, mutual legal assistance procedures are considered too complex, lengthy and resource intensive, and thus too inefficient.”).

[378] Eugenia Lostri, “The CLOUD Act,” *CSIS Strategic Technologies* (blog), October 2, 2020, https://www.csis.org/blogs/strategic-technologies-blog/cloud-act.

[379] Interview with an investigator abroad on February 27, 2024.

[380] Office of International Affairs, “Regarding CLOUD Act Executive Agreements,” updated September 22, 2023, https://www.justice.gov/criminal/criminal-oia/regarding-cloud-act-executive-agreements; Office of International Affairs, “Cloud Act Agreement between the Governments of the U.S., United Kingdom of Great Britain and Northern Ireland,” October 3, 2019, https://www.justice.gov/criminal/criminal-oia/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern; Office of International Affairs, “Cloud Act Agreement Between the Governments of the U.S. and Australia,” December 15, 2021, https://www.justice.gov/criminal/criminal-oia/cloud-act-agreement-between-governments-us-and-australia.

enforcement may be reluctant to investigate a report where the content is from nine or more months ago,[381] but some countries have more stringent privacy protections that preclude the lengthy preservation of data—and may even impede its initial collection. For example, in the European Union, companies' legal ability to voluntarily scan for CSAM required the passage of a special exception to the EU's so-called "ePrivacy Directive".[382] Plus, against a background where companies are supposed to retain personal data no longer than reasonably necessary,[383] EU member states' data retention laws have repeatedly been struck down on privacy grounds by the courts[384] for retention periods as short as four or ten weeks (as in Germany) and as long as a year (as in France).[385] As a result, even if a CyberTipline report had an IP address that was linked to a specific individual and their physical address at the time of the report, it may not be possible to retrieve that information after some amount of time.

Law enforcement agencies abroad have varying approaches to CyberTipline reports and triage. Some law enforcement agencies will say if they get 500 CyberTipline reports a year, that will be 500 cases. Another country might receive 40,000 CyberTipline reports that led to just 150 search warrants. In some countries the rate of tips leading to arrests is lower than in the U.S.[386] Some countries may find that many of their CyberTipline reports are not violations of domestic law. The age of consent may be lower than in the U.S., for example. In 2021 Belgium received about 15,000 CyberTipline reports, but only 40% contained content that violated Belgium law.[387]

7.11.2 Challenges in lower-income countries

The challenges in lower income countries are particularly severe. In some African countries law enforcement lack decent computers and good internet connections and even gas for vehicles to execute search warrants. In one African country, senior law enforcement officials are uncomfortable making a decision about ignoring CyberTipline reports with viral images, so there is an inability to triage. In some countries law enforcement may have to pay online platforms for certain

[381] Interview with a law enforcement officer on August 18, 2023.
[382] Tar, "Commission highlights data shortfall in interim child sexual abuse regulation."
[383] "For how long can data be kept and is it necessary to update it?," The European Commission, accessed February 21, 2024, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_en.
[384] Luca Bertuzzi, "Europe seeks a way out of the data retention pickle," *The Privacy Advisor* (blog), *International Association of Privacy Professionals*, November 29, 2022, https://iapp.org/news/a/europe-seeks-a-way-out-of-the-data-retention-pickle/; "Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources," Global Freedom of Expression, April 8, 2014, https://globalfreedomofexpression.columbia.edu/cases/ecj-digital-rights-ireland-ltd-v-minister-for-communications-marine-and-natural-resources-c%E2%80%9129312-and-c%E2%80%9159412-2014/.
[385] Thomas Wahl, "CJEU: German Rules on Data Retention Not in Line with EU Law," *Eucrim*, November 15, 2022, https://eucrim.eu/news/cjeu-german-rules-on-data-retention-not-in-line-with-eu-law/; Judgment of the Court in Joined Cases C-339/20 | VD and C-397/20 | SR, Sept. 20, 2022, https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-09/cp220157en.pdf.
[386] Interview with an employee of a company that creates software for law enforcement on August 15, 2023.
[387] The AviaTor Project, "Save Time, Save Lives."

pieces of information, and they may not have a budget for that expense. One respondent noted, "If you have a tool you can't read [referring to the fact that CyberTipline reports are in English] and you are overworked, it's hard to motivate people to work on this stuff."[388] In some African countries law enforcement face "every obstacle possible."[389] Many of the challenges that we heard about are likely relevant to all sorts of criminal investigations.

We interviewed two individuals in Mexico who outlined a litany of obstacles to investigating CyberTipline reports even where a child is known to be in imminent danger. Mexican federal law enforcement have a small team of people who work to process the reports (in 2023 Mexico received 717,468 tips[390]), and there is little rotation. There are people on this team who have been viewing CyberTipline reports day in and day out for a decade. One respondent suggested that recent laws in Mexico have resulted in most CyberTipline reports needing to be investigated at the state level, but many states lack the know-how to investigate these tips. Mexico also has rules that require only specific professionals to assess the age of individuals in media, and it can take months to receive assessments from these individuals, which is required even if the image is of a toddler.[391]

The investigator also noted that judges often will not admit CyberTipline reports as evidence because they were provided proactively and not via a court order as part of an investigation. They may not understand that legally U.S. platforms must report content to NCMEC and that the tips are not an extrajudicial invasion of privacy.[392] As a result, officers may need a court order to obtain information that they already have in the CyberTipline report, confusing platforms who receive requests for data they put in a report a year ago. This issue is not unique to Mexico; NCMEC staff told us that they see "jaws drop" in other countries during trainings when they inform participants about U.S. federal law that requires platforms to report CSAM.[393]

Another barrier related to CyberTipline reports received by other countries is that the form data is in English. In the NCMEC Case Management Tool for law enforcement, the field names are available in English, Spanish, French, German, Portuguese, Arabic, Hindi, and Thai, but the content of the tips is generally provided in English as submitted by the platforms.[394] Foreign law enforcement may not know English, and may need to copy and paste parts of the report into an online translator to simply read the content.[395] One respondent, discussing this issue in a non-English speaking African country, said that the lack of report translation "doubles or triples the effort" needed by law enforcement.[396]

There are a number of interesting interventions to increase the motivation and capacity of law enforcement abroad to assess and investigate CyberTipline reports.

[388] Interview with an NGO employee on October 10, 2023.
[389] Interview with an NGO employee on November 15, 2023.
[390] NCMEC, "2023 CyberTipline Reports by Country."
[391] Interview with an investigator in Mexico on August 30, 2023.
[392] Interview with an investigator in Mexico on August 30, 2023.
[393] Interview on September 28, 2023.
[394] NCMEC, "CyberTipline 2023 Report."
[395] Interview with an investigator in Mexico on August 30, 2023.
[396] Interview on January 12, 2024.

International Justice Mission partners with NCMEC to run intensive trainings with law enforcement abroad that include almost a year of weekly mentorship.[397] Other governments and organizations have contributed to or participated in these trainings as well.[398]

[397] NCMEC, "Online child abuse has no borders - NCMEC training out of Africa," 2022, https://perma.cc/CS2K-6F8R.

[398] Department of State, "TIP Office Project Descriptions," 2024, https://perma.cc/UVL5-6EXB.

8 Discussion and recommendations

The CyberTipline process exhibits a “hot potato” dynamic. Online platforms report a substantial volume of content that will not and should not be prosecuted, such as memes and viral outrage shares. This might be perceived as over-reporting, but platforms are adhering to legal requirements to avoid the risk associated with neglecting to report any apparent CSAM they detect. NCMEC is passing everything through to law enforcement, including those reports they understand are not actionable, again wanting to abide by the law, and like everyone, not wanting to be responsible for failing to forward a report that could have led to the rescue of a child. This leaves law enforcement with a high volume of tips of widely varying quality.

The process is also marked by an abundance of caution. NCMEC, for example, harbors concerns about the adoption of automatic translation for reports, apprehensive of impactful translation errors. While such concerns are justified, the overwhelming number of reports flooding into other countries—and the considerable benefits that could come from translating these reports—warrants an assessment of these trade-offs and potential mitigating strategies. Platforms are hesitant to detail their suspicions about possible behaviors in CyberTipline reports, worried that inaccuracies in their internal investigations could complicate the work of law enforcement and prosecutors. However, considering the strain even U.S. law enforcement faces due to the sheer volume of reports, there may be value in sharing these educated guesses, albeit with clear disclaimers. Finally, NCMEC, law enforcement, and platforms are all scrupulous about maintaining the independence of platforms’ actions in looking for CSAM on their services, out of an abundance of deference to Fourth Amendment considerations.

There are no easy solutions to address some of the large structural issues with the process. No one, for example, suggested modifying laws to exempt platforms from reporting memes and outrage shares because this would increase the risk of missing an important tip. The idea of platforms choosing to review all CSAM before reporting is contentious; although it would aid law enforcement in prioritizing reports, it would slow down the reporting process. It also raises ethical concerns about obligating private sector employees to view CSAM. Altering legislation so that NCMEC is not required to forward all domestic reports to law enforcement also poses risks. More broadly, NCMEC and the CyberTipline system are entrenched enough to endure whether or not these major structural issues get remediated: the system has grown so much in scale, and become so centrally important to combating child sexual exploitation and abuse worldwide, to the point that it has become “too big to fail.”

However, as we will describe in Section 8.1, there are practical measures that stakeholders can implement, which offer minimal drawbacks, to streamline the triage process for law enforcement and ultimately increase the rescue of children and identification of hands-on offenders. Platforms could complete the CyberTipline form more carefully, labeling content as potential memes or viral whenever possible, and providing information on the "who/what/where/when" of the file. They can also bolster their investigative teams focusing on the most egregious offenders on their platforms, providing more comprehensive reports on these cases, thereby enhancing the likelihood of law enforcement action. NCMEC could prioritize improving the technology infrastructure supporting the CyberTipline, including thinking about how reports could be enriched with external data to give law enforcement more signals about whether a tip should be prioritized. Police departments should ensure they are sufficiently prioritizing investigations into online crimes against children, and all local law enforcement agencies should affiliate with ICAC Task Forces. Both NCMEC and Task Forces should partner with qualified academics to provide more transparency on internal reporting flows, internal tipline data, and bottlenecks to prosecution.

Many professionals in this field have grown weary of the narrative that emphasizes the large topline number of "36 million CyberTipline reports in 2023," as the significance of this figure remains unclear. On the one hand, this number might overstate the threat, considering it includes numerous reports depicting non-malicious shares. On the other hand, every interviewee we spoke with who had an opinion on the matter believed that the threat of online crimes against children is actually underestimated. They argued that due to the prevalence and severity of these crimes, they should receive greater prioritization. One respondent critiqued the over-reliance on the 30+ million statistic, expressing that it fails to effectively convey the seriousness of the issue: "We aren't doing a good enough job of selling the threat [...] The number gets trotted out to justify everything, and then people wonder why they don't get resources."[399] Partnering with academics would help bring empirics to some of this, bringing insights into the relationship between CyberTipline reports, arrests, and victim identification.

8.0.1 The Coming Wave of AI-Generated CSAM

Our interviews occurred during a critical time, as generative AI technologies emerged that allow individuals with basic technical skills to create photo-realistic CSAM locally or using online services. As our team members have shown in previous work, groups of hundreds of individuals working together have been able to retrain and tune open-source models, such as Stable Diffusion, to create CSAM.[400] These models are distributed in relatively large chat rooms or are used to create commercial web services that create CSAM for small cryptocurrency payments. These services threaten to flood the CyberTipline and downstream law enforcement with millions of new images that cannot be clustered with images from real children or matched with existing CSAM using perceptual hashes. Recently, NCMEC experienced its first "million report day" due to a

[399] Interview with a federal civil servant on October 24, 2023.

[400] David Thiel, Melissa Stroebel, and Rebecca Portnoff, "Generative ML and CSAM: Implications and Mitigations," *Stanford Digital Repository*, June 24, 2023, https://doi.org/10.25740/jv206yg3793.

widely shared viral meme, and dealing with that volume was only possible due to automated clustering.[401] One million unique images reported due to the AI generation of CSAM would be unmanageable with NCMEC's current technology and procedures.

Beyond the increase in volume, generative AI introduces many complexities to the CyberTipline process. With the capability for individuals to use AI models to create CSAM, there is concern that reports of such content—potentially indistinguishable from real photos of children—may divert law enforcement's attention away from actual children in need of rescue.[402] NCMEC highlighted numerous instances, however, where it was critical to escalate reports involving generative AI to law enforcement. These included AI-generated CSAM based on real photos of children to which the individual had access and AI-created images used in sextortion schemes.[403]

We have only begun to see the impact of AI on the child safety ecosystem, and it is clear that a serious, coordinated effort between platforms, NCMEC, law enforcement and Congress is necessary to just maintain the current efficacy of the CyberTipline system.

8.1 Recommendations

8.1.1 Platforms

Online platforms that host user-generated content are on the front lines of identifying, preventing, and reporting child sexual exploitation material through the CyberTipline. Some of these are legal obligations, but determining how to identify and submit content is largely platforms' decision. Platforms must ensure that illegal content that harms children is discovered, that tips are as informative as possible and can be easily processed, and that evidence retention is secure and available for investigations. Dedicated trust and safety staff are best positioned to investigate activity on their platforms and develop detection methodologies that adapt to new behaviors. There is no substitute for such investigations.

Therefore, we recommend the following actions by online platforms and industry coalitions:

- **Prioritize child safety staffing** with expertise for in-depth investigations that proactively identify and address child sexual abuse and exploitation to stay ahead of measures taken by bad actors to avoid detection.
- **Join the Tech Coalition.** The most basic membership is $10,000 per year and provides access to all member resources and the Tech Coalition community.

[401] Interview with NCMEC staff between January 30 and February 1, 2024.
[402] Thiel, Stroebel, and Portnoff, "Generative ML and CSAM: Implications and Mitigations."
[403] Interview with NCMEC staff between January 30 and February 1, 2024.

- The Tech Coalition should consider **providing informational resources**, including information on what makes a report actionable, to platforms that cannot afford this membership fee and/or submit so few reports that membership might not make sense.

To improve effectiveness in tip transmission, platforms should:

- **Deploy and optimize hash-based CSAM detection tools** with dedicated engineering resources.
- Invest dedicated engineering resources in **implementing the NCMEC reporting API.** Ensure there is an accurate and (where possible) automated process for completing all relevant fields.[404] There are many fields, and while not all are necessary, our interviews suggest reports are more actionable when they provide offender information (including location information, particularly an *upload* IP address), victim information (including location information), the associated file (a hash alone is insufficient) or chat, and the time of the incident (including a field describing how the platform defines the incident time).
  - → Other important fields include the "Potential Meme," "Generative AI," and "File Viewed by Company" boxes. Ensure that the "File Viewed by Company" box is being checked if and only if a human reviewed the file associated with this report.[405] This box should not be checked if a human reviewed the image or video in the past, but not the exact file being included in the report.
- Periodically **audit the accuracy and consistency** of CyberTipline reports, both automated and human-generated.
- Be aware that if a human reviews a file associated with a CyberTipline report, and if the "**File Viewed by Company**" box is accurately checked, this will greatly increase: (1) the ability of NCMEC to identify new victims, (2) the ability of NCMEC to accurately escalate the report, (3) the likelihood that law enforcement will investigate the report, and (4) the ability of law enforcement to accurately triage among reports. Platforms may still have legitimate reasons to choose to not have humans review some or all files, but they should be aware of these tradeoffs.
- Establish and integrate **content provenance and authenticity standards** for the detection of AI-generated media in coordination with ongoing industry efforts coordinated by groups including the Content Authenticity Initiative[406] and Partnership on AI.[407] Use the CyberTipline field signaling the file contains suspected AI-generated content.

[404] "CyberTipline Reporting API Technical Documentation."
[405] We note that although the CyberTipline field says "Generative AI," while the meme field says "Potential Meme," we believe platforms can interpret the "Generative AI" field as potential generative AI, as the API documentation defines this field as: "The file contains content that is believed to be Generative Artificial Intelligence."
[406] https://contentauthenticity.org/.
[407] https://partnershiponai.org/.

- **Maintain dedicated contact information** for NCMEC, including at minimum a dedicated email address. This contact address should not be an individual employee's contact information, given the rapid rate of personnel turnover in child safety roles; rather, it should be an email address such as ncmec@[company].com, childsafety@[company].com, or similar, that routes inbound emails to the specific employee(s) responsible for corresponding with NCMEC.

To increase the likelihood of victims being identified and rescued, platforms should:

- **Safely preserve reported CSAM** and related data beyond the current 90-day requirement to at least 180 days to support more law enforcement investigations.
- **Maintain a law enforcement guide and a law enforcement portal**. Keep the law enforcement guide up to date, including contact information, and have a process for regularly updating the guide and highlighting such changes.
- **Hire a law enforcement outreach officer** to handle law enforcement requests for child safety investigations. This person can respond to general law enforcement questions, for example related to platform data variable definitions.

If NCMEC gains legal authorization to use cloud services and short-term technical contractors, the large platforms should:

- Provide technical assistance by **loaning engineers and product managers** to help re-architect and uplift the CyberTipline into the cloud.
- Provide **low-cost or free cloud services** wherever possible.

8.1.2 NCMEC

As the organization responsible for the CyberTipline, there are several changes that NCMEC can make to increase the efficacy of its technology and the likelihood of successful prosecutions.

We recommend NCMEC prioritize the following improvements, which could be part of a two-year project specifically funded by Congress. Some of these projects would be easier with legislation enabling NCMEC to transfer CyberTipline report data to cloud services, though with sufficient technical resources access to cloud services is not strictly necessary. As with all of our funding-related recommendations, Congress should not take these funds from the ICAC Task Forces, which are very resource-constrained.

- Invest additional engineering resources in the **automated deconfliction process**. NCMEC is best-placed to do this work as they are the only entity with both cross-platform and cross-jurisdiction visibility. By more effectively identifying similarities in CyberTipline reports (beyond existing entity matching work) this will ensure tips linked to the same offender are not unnecessarily distributed across jurisdictions and to allow law enforcement to more easily batch tips.

- Consider building a **JSON-based reporting API**, to replace or operate alongside the current SOAP API. A JSON-based API will be simpler to integrate with and more familiar to younger developers.
- Use an increase in funds to expand and **offer competitive salaries** to technical division staff. With funding constraints, a fellowship program could help expand resources for the technical division, as modeled by the U.S. Digital Service program for federal agencies.
- **Create an employment model** that allows employees from partner tech companies to serve 6–12 month rotations on NCMEC's technical team. This could be especially helpful during the initial project to securely re-architect and refactor NCMEC's existing services to run on a cloud service provider.
- Publish a **negative hash set** of images that have been reported as CSAM but have been verified to not be violative, possibly because the subject has been verified to have been an adult at the time the image was created. This would allow platforms to stop reports (and automated processes such as account termination) on known legal content.
- Create a prominent and easily accessible section of the NCMEC website focused on onboarding online platforms. **Provide clear information** on how platforms can reach out to NCMEC to get started reporting via the API.
- Integrate the NCMEC-commissioned API to **match CyberTipline report IP addresses** with data from peer-to-peer file sharing sites to allow law enforcement to more accurately identify high risk offenders.
- **Continue the development of APIs** that will facilitate CyberTipline report enrichment to help law enforcement more accurately triage tips. This should include the creation of a LikelyCompromisedAccount flag that could be set by platforms that detect password changes or other indications of compromise.
- Continue to **prioritize the old file review process** that will facilitate triage for files that NCMEC staff cannot view.
- Continue to **create new internal tooling** that will give NCMEC analysts the same automated capabilities available to platform child safety investigators. One example would be a system to automatically resolve screen names against publicly available social media profiles, a process that is currently done with manual searches across dozens of platforms.
- Provide a **dedicated field and standard structured data format** for platforms to submit chat text and associated metadata.

On the platform engagement front, NCMEC should:

- **Provide more information to platforms** about the value of their CyberTipline reports. Even one set of feedback per platform, once a year, explaining what aspects of that platforms' reports were useful, and how they could be improved, would be enormously beneficial. While this feedback might be currently provided to large platforms, this feedback would be particularly useful to the long tail of platforms that only submit a small number of reports annually. Our interviews suggest these platforms find it demotivating to never receive any follow up from law enforcement along with no feedback from NCMEC.

- **Provide detailed briefings** to platforms about observed shifts in tactics related to online-facilitated crimes against children. These briefings should be targeted at platform staff who specialize in investigating these crimes. Consider inviting platforms beyond the highest-volume reporters.

On the academic engagement front, NCMEC should:

- **Create further partnerships** that invite qualified academic researchers to analyze reporting flows and internal tipline data. The use of AI to detect and prioritize CSAM is a great example of cutting-edge research that academic groups would be motivated to perform but unable to do without the help of NCMEC.
- **Consider facilitating foundation-funded research competitions** to meet CyberTipline product needs. Guided competitions have a long history[408] of rapidly accelerating applied research in fields and there is an opportunity for NCMEC to create a new academic community around online child safety.

There are normative questions related to the extent to which NCMEC should be prioritizing domestic CyberTipline reports. Some respondents think NCMEC—which is already stretched thin—should focus on the U.S. "It's too much for NCMEC to handle this for the whole world," one law enforcement officer said.[409] Others think NCMEC should have a broader mandate to do more to support law enforcement abroad. Some believe there should be a small number of regional bodies that NCMEC automatically passes tips to, and those bodies should analyze/triage the non-U.S. tips. We do not weigh in on that question, but at minimum it seems like an automated translation process for both the CyberTipline report template and fields would provide great payoffs abroad. We believe the potential mis-translation risks are outweighed by the benefits of easing the burden on foreign law enforcement. Additionally, NCMEC receives feedback on how to improve their Case Management Tool from law enforcement. They currently prioritize feedback from U.S. law enforcement, which is understandable from our perspective. If there were other regional organizations to help process CyberTipline reports, there might be capacity to accommodate country-specific requests such as prioritizing reports if a certain word is used, as there is country-level variation in which words could indicate great risk to a child.

8.1.3 Regulatory and legislative responses

Lawmakers at the state and federal levels can introduce legislation to improve CyberTipline functioning:

[408] See the DARPA Grand Challenge or NIST Post-Quantum Cryptography as examples

[409] Interview on August 25, 2023.

- Congress should **increase NCMEC's budget** to enable it to hire more competitively in the technical division, and to dedicate more resources to CyberTipline technical infrastructure development. As a nonprofit, NCMEC will not be able to compete with industry on salaries for engineers, but ideally they could offer salaries at a level that are attractive when combined with the group's mission.
- Congress can **alleviate legal confusion** about child exploitation investigations on the part of other stakeholders. Some platforms, for example, fear that they may face legal liability for retaining CSAM past the mandated holding period, and as law enforcement interviewees noted, this results in the loss of material for investigations. Cloud providers are unwilling to provide services to NCMEC for fear of liability issues. Some of these issues are addressed by the REPORT Act.[410]
- Lawmakers have the power to **transform how law enforcement engages with and prioritizes child safety investigations**. State governments may mandate that every police academy conduct trainings on how to take a cybercrime report. At a federal level, Congress should ensure that ICAC Task Forces have resources to train affiliates.
- **Extend the retention period** for electronic service providers to safely preserve reported CSAM from 90 days to at least 180 days.
- Beyond the statutory preservation period, **authorize platforms to voluntarily preserve reported material** for an additional defined time period, solely for purposes of combating child sexual exploitation and abuse.
- State legislatures and Congress can **clarify applicable law and penalties** for emerging forms of CSAM, such as AI-generated CSAM (consistent with constitutional requirements).[411]

8.1.4 Law enforcement

Our recommendations for law enforcement include:

- Local law enforcement agencies should **affiliate with their ICAC Task Force**.
- Department chiefs should ensure they are **prioritizing the investigation of crimes against children**.
- Department chiefs should ensure they are using technological products for **officer wellbeing** and go through training on crimes against children to understand and properly resource for these crimes.
- Law enforcement agencies should attempt to provide—at minimum—**more information to platforms** about the outcomes of their CyberTipline reports.

[410] REPORT Act.

[411] Riana Pfefferkorn, Addressing Computer-Generated Child Sex Abuse Imagery: Legal Framework and Policy Implications, Feb. 5, 2024, https://www.lawfaremedia.org/article/addressing-computer-generated-child-sex-abuse-imagery-legal-framework-and-policy-implications.

- ICAC Task Forces should **partner with researchers** to provide more transparency about what happens once CyberTipline reports get to law enforcement, including how many reports are investigated, how many lead to prosecutions and what bottlenecks exist.

8.1.5 Education

Though largely beyond the scope of this report, our interviews repeatedly brought up the need for greater public education about online child exploitation—particularly as AI-generated CSAM, self-generated CSAM, and financial sextortion increasingly comprise a larger percentage of CyberTipline reports. Improvements to the CyberTipline will only address harms after they have occurred. Schools, which now find themselves having to address incidents of students creating non-consensual sexual imagery of fellow students using readily-available AI generation apps,[412] should consider educating students about laws as well as reporting processes. Schools should also consider offering online safety training for children and parents on issues such as sextortion. These trainings should occur in the years before children are at greatest risk. A former ICAC Task Force officer described "not my child syndrome," where parents are reluctant to attend trainings because they think their child would never fall victim to these crimes.[413] Schools should think about how to incentivize parent participation.

8.2 Conclusion

In summary, we found that for a platform, initiating a system to detect and report CSAM is a challenging endeavor. We found that platforms face difficult trade-offs in deciding what content to report and how to report it, and that there is wide variation in how platforms choose to work with law enforcement. Moreover, there is a significant disparity in the resources allocated by platforms to address child sexual exploitation issues. We found that NCMEC is improving their CyberTipline technical infrastructure, including important work around deconfliction, yet there remains substantial scope for further improvements. We discussed challenges law enforcement face in triaging and investigating CyberTipline reports. Following these findings, we have proposed a series of policy recommendations aimed at various stakeholders in this domain.

Our most important finding is that it is difficult for law enforcement to triage CyberTipline reports for investigation. Two reports can look very similar, and yet if both were investigated one would lead to someone who was unwillingly spammed with CSAM and the other could lead to the discovery of someone abusing a child. There are many causes of this undesirable status quo: platforms are not investing sufficient resources in completing the CyberTipline report form thoughtfully,

[412] Julie Jargon, "Fake Nudes of Real Students Cause an Uproar at a New Jersey High School," *The Wall Street Journal*, November 2, 2023, https://www.wsj.com/tech/fake-nudes-of-real-students-cause-an-uproar-at-a-new-jersey-high-school-df10f1bb.

[413] Interview on September 22, 2023.

their teams responsible for investigating more severe cases are insufficiently staffed, there is a lack of clarity about what makes for a good report, NCMEC could do more to augment tips with external information, and law enforcement's investigative pace is hindered by the requirement to obtain search warrants to review the content of tips. Stakeholders should prioritize rights-respecting actions that would make it easier for law enforcement to triage.

There are a number of areas for future research:

- What happens to CyberTipline reports? The most effective approach would be for academics to partner with NCMEC to conduct a random sample of tips, potentially stratified by region and filtered to exclude meme content. These researchers could potentially collaborate with ICAC Task Forces and law enforcement agencies abroad to assess the outcome of these reports. Even if researchers could not view reports, they could help Task Forces with a sampling protocol and help develop a protocol for assessing outcomes. While NCMEC provides a helpful 843-page PDF documenting media coverage of "CyberTip Success Stories," including offender arrests,[414] a tracing of a representative sample of CyberTipline reports is the only way to truly understand what happens with most CyberTipline reports.
- We need a deeper understanding of the characteristics of CyberTipline reports. This includes creating cross-tabulations by platform, such as those for memes. Ideally, summary statistics for any non-identifiable information fields from the form should be made publicly available, unless there is a real fear that it would help offenders game the system. This research would require academics to partner with NCMEC.
- The importance of state laws in the U.S. came up repeatedly in our interviews. State laws shape incentives in how to investigate and how and whether to prosecute CSAM cases. Research on the tradeoffs associated with various state laws would be valuable.
- Our research focused on the experiences of law enforcement with substantial experience investigating online crimes against children. Future research could look at the experiences of law enforcement who only investigate a few CyberTipline reports each year.
- With the increasing prevalence of AI-generated CSAM, it is important to study how and when such content is identified as AI-generated. Research should also focus on whether this type of content is overwhelming the CyberTipline and distracting stakeholders from investigating tips that could lead to the rescue of a child, versus when these reports are bringing law enforcement attention to trusted community members who are creating abusive content of children.

Did you notice an error in this report? Email us: shelbygrossman@stanford.edu.

[414] NCMEC, "2023 Media Coverage: CyberTipline Success Stories," 2024, https://perma.cc/ETD7-TU2E.

Stanford | Internet Observatory
Cyber Policy Center

The Stanford Internet Observatory is a cross-disciplinary program of research, teaching and policy engagement for the study of abuse in current information technologies, with a focus on social media. The Stanford Internet Observatory was founded in 2019 to research the misuse of the internet to cause harm, formulate technical and policy responses, and teach the next generation how to avoid the mistakes of the past.