Snap Inc.

The Honorable Charles E. Grassley
Chairman
Committee on the Judiciary
United States Senate
224 Dirksen Senate Office Building
Washington, DC 20510

April 22, 2026

Dear Chairman Grassley:

We are writing in response to your letter dated April 8, 2026 to Evan Spiegel, CEO of Snap Inc., regarding information provided by the National Center for Missing and Exploited Children (NCMEC) and Snap's practices related to reporting to NCMEC's CyberTipline. We appreciate the Committee's oversight on this critically important issue and share the goal of ensuring that reports to NCMEC are as complete, accurate, and actionable as possible to support law enforcement and protect children. The information provided below is based on a review of Snap's records conducted in good faith for the purpose of responding to your request. We have taken reasonable steps to ensure the accuracy and completeness of the information provided.

We would like to take this opportunity to underscore Snap's long-standing commitment to helping protect young people from all forms of online child sexual exploitation and abuse (CSEA). As part of that commitment, we took action in May 2024 to respond to a record rise in CyberTips across the industry,[1] a continued spike in sexual extortion globally, and feedback that we received from law enforcement about the actionability of our CyberTips, by approaching NCMEC about refining and further improving our CyberTip reports. Following consultation with NCMEC, we then implemented a number of internal policy and operational changes designed to increase the value and actionability of our CyberTips while continuing to meet our legal obligation to report. As a result of those efforts, we have materially increased the amount of information provided in our reports to NCMEC. Over time, these efforts have also coincided with a reduction in overall report volume. From a peak of 1.174 million reports in 2024, Snap filed approximately 752,000 CyberTips in 2025, and has thus far submitted over 200,000 reports in 2026. This reflects, in part, refinements to classification and reporting practices informed by feedback from NCMEC and law enforcement regarding how reports are triaged and used.

As explained in this blog post published in August 2025 about our then 15-month CyberTip recalibration process with NCMEC — which continues to this day[2] — Snap's goal is for state, federal, and international law enforcement authorities to confidently pursue CyberTips from Snap because they know our reports can be consistently relied upon as actionable, valuable, and thorough. And, our hope is that those efforts will help

[1] Looking at reporting across industry overall, up until 2024, the annual totals of CyberTips to NCMEC had largely been rising year over year, topping out at a record 36.2 million reports in 2023, up from just over 32 million in 2022, and 4,560 in 1998 when NCMEC's CyberTipline was created.
[2] Snap held a second recalibration session with NCMEC on July 9, 2025, and Snap's third recalibration session with NCMEC is scheduled for April 23, 2026.

prompt a corresponding uptick in related arrests and convictions worldwide. There is always more work to do and more we can improve on, but we are encouraged by the progress we have made over the last two years.

For example, we have significantly improved the reports we label as involving suspected "online enticement."[3] As defined by NCMEC, "Online Enticement involves an individual communicating with someone believed to be a child via the internet with the intent to commit a sexual offense or abduction."[4] We previously used NCMEC's "online enticement" label (which prompts a priority escalation from NCMEC to law enforcement) regardless of whether we identified evidence that the suspect knew or may have known the recipient was a minor. However, based directly on discussions with NCMEC in May 2024 regarding how such reports are defined, assessed, and prioritized, Snap refined its practices. In particular, we updated our approach (1) to take evidence of age knowledge into account when determining whether to apply the "online enticement" label, and (2) to provide additional information relevant to the perceived age of the reported user and victim where appropriate in our CyberTips. These refinements were intended to better align with NCMEC's triage processes and to provide law enforcement with clearer indicators relevant to potential criminal intent, while continuing to report conduct that appears to involve the sexual exploitation of minors. This is just one example of how clear communication and guidance led to meaningful change. Indeed, in the months following the initial recalibration discussion with NCMEC in May 2024, the volume of Snap CyberTips for "online enticement" was reduced by more than 50%, with some cases being reported under other incident types instead. At the same time, those reports that were submitted were more robust.

We understand that NCMEC raised concerns in its March 16, 2026 response to your letter. That response failed to acknowledge the significant progress Snap has made in consultation with NCMEC. It also runs contrary to other positive feedback Snap has received anecdotally from law enforcement regarding our efforts to submit CyberTips that contain higher-quality information and are more actionable. By way of one example, a recent Snap visit to an Internet Crimes Against Children (ICAC) taskforce yielded feedback that a few years ago, perhaps one in five Snap CyberTips may have been actionable by this ICAC taskforce, but now, that ratio averages one in two.

We are committed to continued improvement in all aspects of our safety work. Day in and day out, we are battling whole-of-society issues and we bring a whole-of-*company* approach to bear — with the ultimate twin objectives of mitigating risk and reducing harm. While we disagree with NCMEC's characterization of "significant issues concerning reporting" affecting data quality insofar as they concern Snap's reporting, we share NCMEC's goal of protecting children from these horrific crimes, and we will continue our efforts to further improve our CyberTip reporting in furtherance of it.

1. **Please describe feedback from NCMEC regarding reports you are required to provide pursuant to 18 U.S.C. § 2258A. What changes or policies were developed in response to this feedback? If no changes or policies were implemented, please state so and explain in detail why your company declined to take additional action.**

Since our first recalibration with NCMEC in May 2024 and consistent with evolving NCMEC guidance and industry practices, we have refined our policies, improved data quality and labeling, and enhanced

[3] NCMEC has enumerated certain "incident types," such as "online enticement," that a reporting company may use to categorize a CyberTipline report based on the nature of the suspected CSEA.
[4] NCMEC, *Online Enticement*, https://www.missingkids.org/theissues/onlineenticement.

operational efficiencies, all with the objective of submitting to NCMEC and, ultimately, law enforcement the highest-value CyberTip reports possible. In addition to our annual recalibrations with NCMEC, we confer with NCMEC approximately every other month, and ad hoc as need be, to talk through questions, "edge cases," or outstanding issues that have arisen. We also meet with global law enforcement, including ICAC personnel, and directly solicit feedback in a variety of other settings, including: NCMEC's annual CyberTip Roundtables; our own virtual ICAC Feedback Roundtable; the NorthWest ICAC Conference; Wisconsin ICAC Conference; Crimes Against Children Conference; the Florida Law Department ICAC Conference; and bespoke visits to various ICACs.

In 2024, we gathered feedback from NCMEC, as well as international, federal, and state law enforcement, which indicated that a large percentage of industry CyberTip reports were inactionable. This feedback highlighted that reports were frequently closed due to issues such as imagery where it is unclear whether the person depicted is a minor or an adult ("age indeterminate" content), self-produced imagery shared between minors, and lack of adequate contextual information provided in reports. In response to such feedback and NCMEC's guidance, we implemented several critical internal policy and operational changes that took effect starting in August 2024, including:

- **Clarified Policy Definitions:** We refined our internal policy definitions in part to better align with NCMEC's incident types including "online enticement," "child pornography," "child sexual molestation," "child sex trafficking," and "unsolicited obscene material sent to a minor." For example, as described above, to align with NCMEC's guidance, we took evidence that a reported user knew or may have known they were interacting with a minor into account when classifying reports as involving "online enticement," and we required evidence of first-party content or a live victim for reports classified as "child sexual molestation." This is consistent with NCMEC's guidance on how it triages such reports.
- **Steps to Address Age-Indeterminate Content:** We updated how we evaluate and report content depicting an individual who may not be readily identifiable as a minor. In such cases, we seek to identify specific signals indicating that the individual is a minor, such as the age of the user on record, references to age within a report submitted to Snap, or additional contextual clues, in addition to including such contextual information in our CyberTip reports as discussed below.
- **Steps to Address Minor-to-Minor Interactions:** We created clearer guidance for handling minor-to-minor interactions to better distinguish situations such as the consensual sharing of self-produced imagery or teenage romantic relationships, from those involving evidence of coercion or sextortion, an older minor grooming a younger minor, or a commercial sexual transaction.
- **Enhanced Data Sharing:** To help further law enforcement investigations, we expanded the data provided in our CyberTip reports to include information, when available, such as:
    - Additional subscriber information for the reported user and victim;
    - Upload IP address and source port information for the reported user in certain cases;
    - The apparent source of reported media (for example, whether it was uploaded from the user's camera roll or created using the Snapchat app's camera);
    - Additional information about where reported content appeared on Snapchat and how it was distributed;
    - Information provided by an individual who reported content or an account to Snap in additional cases;
    - Method of detection (whether hash-match, automated, or reported) used for content provided in a CyberTip; and

    - Additional contextual information about how Snap determined whether the reported user and victim appeared to be an adult or minor.

These changes increased the overall amount of data provided in our reports to NCMEC. At the same time, while continuing to fulfill our legal obligation to report CSEA in CyberTips, our overall report volume decreased. We also submitted fewer reports labeled as "online enticement," while submitting a greater percentage of reports labeled with incident types identified by NCMEC as lower priority such as "unsolicited obscene material sent to a minor," helping NCMEC and law enforcement to better prioritize cases. We apprised NCMEC of these updates at our second recalibration session held in July 2025.

Throughout 2025, we continued to solicit guidance from NCMEC and law enforcement, including ICAC Commanders, on the actionability of our CyberTip reports. This feedback highlighted that, industry-wide, evidence of "age knowledge" and criminal intent was often missing from CyberTips, and age-indeterminate content remained an issue. On the other hand, information provided in CyberTips such as source port data and multiple lines of chat messages (when a chat message was reported) proved very helpful. NCMEC also noted that using certain "annotations" they had developed to help identify the nature of the suspected CSEA reported in a CyberTip was useful to assist them in triaging and prioritizing reports. In response, we have implemented further updates, including:

- **Stricter Age-Knowledge Requirements:** Consistent with guidance from NCMEC, we updated our internal policies to take into consideration evidence regarding the reported user's knowledge of the victim's age for additional types of reports. For certain types of "online enticement" reports, such as sextortion or non-consensual intimate imagery (NCII) involving a minor, we began indicating in our reports *whether* such evidence was included, in order to assist NCMEC and law enforcement in triaging and prioritizing such cases.
- **Report-Level Annotations:** We began using new report-level annotations provided by NCMEC. These include indicating when a report pertains to "sextortion," "sadistic online exploitation," and a "minor-to-minor interaction."
- **Further Enhanced Data Sharing:** We have further expanded the data we provide in our CyberTip reports, including, when available:
    - Source port information in the majority of cases;
    - More lines of reported Chat messages;
    - Additional context about the reported user's knowledge of the victim's age;
    - Content provided on the reported user's public profile;
    - Information about the reported user's device; and
    - Geolocation data.

Our third recalibration with NCMEC will take place on April 23, 2026, where we will once again present NCMEC with updates to our internal policies and CyberTip reporting processes, solicit their feedback on these changes as well as anticipated trends and problems they may face, and work through complex and challenging cases together.

We know this work on our CyberTip reporting will never be finished, and that the landscape affecting it will continuously change. The feedback loop we have created with NCMEC and law enforcement has enhanced, and will continue to enhance, the quality and actionability of our CyberTip reports.

2. **What steps has your company taken to improve child exploitation reporting in 2026? If none, why not?**

We refer to the information provided in our response to Question 1. A number of the changes made following our second recalibration session with NCMEC occurred earlier this year, including the implementation of the new report-level annotations, and the inclusion of new types of data in our CyberTips. We have also continued to solicit feedback from NCMEC and law enforcement about our CyberTips, and scheduled our third recalibration session with NCMEC.

In addition, we highlight that in 2026 Snap has launched a project to reassess our overall process for receiving and responding to reports of safety concerns, including (but not limited to) CSEA, on Snapchat. The goal of this process is to further improve our overall reporting system, better enabling users and others to submit reports when appropriate and better enabling us to effectively take action on such reports (including by submitting CyberTips for cases involving CSEA). A key component of that effort has been gathering inputs and feedback at two workshop-type sessions held in February 2026: one with members of our Safety Advisory Board (SAB) on February 23, 2026 (virtual), and a second with a group of child and online safety experts, including several focused on CSEA in particular on February 26, 2026 (hybrid - virtual and in-person at Snap's Washington, D.C., office).[5] We have also leveraged various other inputs for this broader internal workstream this year.

3. **What steps has your company taken to improve location information provided to NCMEC? If none, why not?**

Snap has taken, and continues to take, affirmative steps to enhance our CyberTip reports with key data intended to help NCMEC and law enforcement locate reported suspects and victims quickly and reliably. Snap CyberTips include phone numbers with area and country codes, when available, to support identification and location efforts. Our CyberTip reports also include IP address information that, since 2024, we have enriched with additional IP data sources to increase accuracy and usefulness. Following direct feedback from both NCMEC and law enforcement, Snap began including upload IP address information for certain categories of content in 2024 and is actively working to expand the scope of these efforts. Also in 2024, after law enforcement advised us that source port data was becoming critical to locating offenders, Snap began implementing updates to provide source port data in our CyberTips. As of the date of this letter, Snap consistently provides source port data in more than 90% of its CyberTips.

In addition, we recently augmented our CyberTip reports by providing latitude and longitude coordinates for the reported user when such data is available from the user's device. These updates reflect our ongoing commitment to improving the robustness and operational value of the information we provide to NCMEC and law enforcement.

We appreciate the opportunity to address your questions, and look forward to further opportunities to engage with the Committee on this topic.

//

[5] A NCMEC official was invited to the session at Snap's office, but after Snap provided additional requested background material about the session, no RSVP from NCMEC was received.

Sincerely,

Gina Woodworth
Sr. Director, Americas Public Policy