Question for the Record from Senator Sheldon Whitehouse
U.S. Senate Committee on the Judiciary
"Protecting Our Children Online"
Submitted on March 7, 2023

Response from Ms. Michelle DeLaune
(President and CEO, National Center for Missing & Exploited Children)

Question 1: Please describe your preferred legislative changes, if any, to the federal immunity granted under Section 230 of the Communications Decency Act of 1996 (47 U.S.C. § 230).

NCMEC Response: As the congressionally-designated clearinghouse and national resource center on missing and exploited children issues, NCMEC views proposed legislative changes to Section 230 from the narrow lens of the statute's impact relating to online child sexual exploitation. The immunity granted to online platforms under Section 230 historically has been interpreted to limit the ability of children victimized by online sex trafficking and the online distribution of child sexual abuse material (CSAM) in which they are depicted from seeking recourse against all entities who participated in their harm – including online platforms that knowingly facilitated their sexual exploitation online. This expansive interpretation of the immunity provided under Section 230 has led to the dismissal of dozens of lawsuits brought by children and their families against online platforms that were aware that CSAM was distributed on their platforms and facilitated or enabled posting of this content or refused to remove content and/or user accounts responsible for distributing the content. As a result, children who have been sexually exploited online are left with no legal recourse and denied their day in court against any online platform, regardless of the platform's knowledge, culpability, or affirmative participation in the child's sexual exploitation online.

In 2018, Congress moved to address Section 230's expansive application in child sex trafficking suits by passing the Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (FOSTA) (Public Law No. 115-164). This law amended Section 230, for the first time since its enactment in 1996, to specifically allow civil actions and state criminal prosecutions to be brought against online platforms for sex trafficking violations.[1]

NCMEC proposes an additional legislative change to Section 230 modeled on FOSTA to enable children and their families to bring civil actions and state prosecutors to bring state criminal

[1] 47 U.S.C. § 230(e)(5).

prosecutions against online platforms that knowingly facilitate the distribution of CSAM online. Similar to FOSTA, this narrow legislative revision would clarify that Section 230's immunity from civil causes of action and state prosecutions does not extend to online platforms that violate child pornography federal and state laws. The EARN IT Act, which is pending re-introduction, contains a provision that would encompass this legislative change to Section 230 that NCMEC endorses. The introduction and passage of the EARN IT Act would fulfill the central legislative changes to Section 230 that NCMEC proposes in order to ensure that children victimized by the online distribution of CSAM in which they are depicted are empowered with legal resource against online platforms that knowingly facilitate and engage in the distribution of CSAM online.

Questions for the Record from Senator Thom Tillis
U.S. Senate Committee on the Judiciary
"Protecting Our Children Online"
Submitted on March 7, 2023

Responses from Ms. Michelle DeLaune
(President and CEO, National Center for Missing & Exploited Children)

Question 1: As you know, in 2021, NCMEC's cyber tipline received 29 million reports of suspected online child sexual exploitation- child sexual abuse material (CSAM). Out of those 29 million reports, how many were evaluated by law enforcement and how many led to convictions?

NCMEC Response: NCMEC is required by federal law to make reports submitted to the CyberTipline available to law enforcement. See 18 U.S.C. § 2258A(c). All CyberTipline reports are made available to international, federal, state, or local law enforcement agencies for their independent review and potential investigation. As a nonprofit organization, NCMEC does not have investigative authority or capabilities and does not have insights into the investigative and prosecutorial evaluations and decisions that are made regarding CyberTipline reports. NCMEC devotes significant resources towards assisting in the triage and prioritization of CyberTipline reports in an effort to elevate critical reports that have a high likelihood of child sexual exploitation. However, NCMEC is not involved in law enforcement's review and evaluation of CyberTipline reports or in decisions relating to which reports law enforcement may choose to investigate and which reports ultimately lead to the filing of criminal charges, including potential prosecution and adjudication of child sexual exploitation charges. NCMEC also has no legal standing or official authority to gain independent knowledge of how many CyberTipline reports law enforcement evaluates or how many reports lead to convictions in international, federal, or state criminal court proceedings. Additionally, there is no statutory requirement for law enforcement to provide feedback or metrics to NCMEC relating to the number of CyberTipline reports they evaluate and the number of reports that lead to a judicial adjudication, including convictions.

While NCMEC has no authority to require law enforcement to provide feedback relating to CyberTipline reports, and there is no legal requirement for law enforcement to provide such feedback, NCMEC has implemented several layers of substantive protocols to obtain feedback from law enforcement relating to their handling of CyberTipline reports. NCMEC encourages and facilitates the submission of feedback by law enforcement relating to CyberTipline reports via email, phone, NCMEC's Law Enforcement

Services Portal,[1] NCMEC's Case Management Tool,[2] the ICAC Data System (IDS),[3] and other feedback tools utilizing law enforcement web services. In addition to enabling users to provide feedback on CyberTipline reports directly through NCMEC's Case Management Tool, NCMEC enables administrators to set auto-reminders to provide feedback and regularly emphasizes the importance of providing feedback to NCMEC at its trainings for law enforcement.

NCMEC's feedback system contains numerous structured fields and free text fields for law enforcement to provide feedback on reports they have received. The following are examples of the feedback NCMEC requests from law enforcement through its feedback system:

Case Status (Conviction; Arrest; Ongoing Investigation; Referred; Closed)

If ARREST: Did you identify a child victim (Yes; No)

If ARREST: Did you identify any additional victims? (Yes; No). How many?

If CLOSED: Please indicate the reason(s) for closing the report (Unable to locate subject; ESP legal response does not contain information; No crime committed; No prosecutorial merit; Alleged child is an adult; Age of child victim is unable to be determined; False Report; Unfounded; Person or User Reported is deceased; Other)

If CLOSED: Does this case involve self-production (Yes; No). Have you identified the child victim? (Yes; No)

Was the information provided by NCMEC useful? (Yes; No)

If NO: Please indicate the reason(s) the information was not helpful (State information; Limited Information; Other)

Feedback from law enforcement can provide valuable insights for reporting ESPs and allows NCMEC to consider improvements to the CyberTipline's efficiency. Despite the importance of receiving feedback and NCMEC's substantive efforts to facilitate law enforcement's submission of feedback on CyberTipline reports, most agencies provide little or no feedback. It is not uncommon for NCMEC to learn of CyberTipline outcomes from news articles and media inquiries, instead of from law enforcement directly. To date,[4] for the 29.3 million CyberTipline reports NCMEC made available to law enforcement in 2021, law enforcement has submitted feedback relating to only 262,654 reports. The chart below shows the case status provided by law enforcement in the feedback that was submitted relating to CyberTipline reports made available to them in 2021:

[1] https://lesp.ncmec.org/LESP/login.

[2] Some international, federal, and state/local law enforcement agencies use the Case Management Tool, NCMEC's data management interface, to download CyberTipline reports made available to them.

[3] Some ICACs use IDS, another data management tool, to download CyberTipline reports made available to them.

[4] Investigation and prosecutorial times for CyberTipline reports can vary tremendously depending on law enforcement capacity; the complexity of the investigation; prosecutorial delays, etc. As a result, it is not unusual for charges relating to a CyberTipline report to be prosecuted years after the report was made available to law enforcement. When this occurs, it diminishes the probability that NCMEC will receive feedback relating to the CyberTipline report and also extends the timeframe within which feedback information may be submitted by law enforcement.

LE Case Status	Distinct Reports
Arrest	12,847
Closed (law enforcement determined case had no prosecutorial merit or was unfounded; investigation could not proceed due to ESPs' failure to retain data; case related to self-produced images/videos)	202,108
Conviction	61
Ongoing Investigation	47,570
Referred to Another Law Enforcement Agency	68
Total	**262,654**

Question 2: Did you see an increase of suspected online child sexual exploitation-CSAM reports in 2022?

NCMEC Response: Yes, NCMEC saw an increase in reports relating to suspected online child sexual exploitation-CSAM in 2022. In 2021, NCMEC received 29.3 million CyberTipline reports containing over 84.9 million images, videos and other content relating to child sexual exploitation. In 2022, NCMEC received over 32.3 million CyberTipline reports containing over 88.3 million mages, videos, and other content relating to child sexual exploitation.

Question 3: With NCMEC being the nation's largest child protection organization, NCMEC also works with social media platforms. Are social media platforms and websites reporting online child sexual exploitation-CSAM? If not, what steps can social media platforms do to improve the reporting efforts?

NCMEC Response: Some social media platforms and websites are reporting online child sexual exploitation-CSAM to NCMEC, however the reporting is largely voluntary, inconsistent, driven by just a handful of large companies, and prone to gaps and delays that complicate NCMEC's handling of reports, law enforcement's potential investigation, and ultimately the identification and recovery of children from sexually abusive situations. Current law requires online platforms defined as electronic service providers (ESPs) to submit a report to NCMEC's CyberTipline when they have actual knowledge of a violation of federal child pornography laws on their platforms. See 18 U.S.C. §2258A. Online platforms are not required to take proactive steps, including use of free technology tools and initiatives, to detect child sexual exploitation content, remove content after it has been reported, or submit substantive, consistent content in CyberTipline reports. Additionally, there are no legal requirements regarding what information an online platform must include in a CyberTipline report, and many companies routinely fail to include substantive or actionable information in their reports. In 2022, 4% of CyberTipline reports contained so little information regarding the geographic location of the incident being reported that it was not possible for NCMEC to determine where in the world the offense had occurred. Similarly, in 2022, NCMEC categorized just over 50% of all CyberTipline reports as "informational", rather than "actionable". A CyberTipline report is categorized as "informational" when the reporting company has not provided sufficient information to determine the nexus to child sexual exploitation or the company is reporting a historical incident, rendering the reported information stale,

or the report contained viral imagery that was being circulated at high volumes over a short period of time due to outrage by online users or in an attempt to help rescue the child.

While approximately 1,500 ESPs were registered to report to the CyberTipline as of January 31, 2023, only 236 companies submitted reports in 2022, and of these, 5 companies accounted for 93% of all CyberTipline reports submitted.

There are many improvements that can be legislatively required or voluntarily undertaken by online platforms to improve reporting efforts. NCMEC is in favor both of legislative efforts to improve reporting to the CyberTipline and continued efforts to work with technology companies to improve their reporting. The following is a list of reporting improvements that NCMEC recommends and supports:

- Mandatory reporting of child sex trafficking and sexual enticement of a child – currently online platforms are not required to report instances of child sex trafficking or the sexual enticement of a child to the CyberTipline. These two crimes must be added to the list of child sexual exploitation crimes that ESPs must report to the CyberTipline. The EARN IT Act, which is pending re-introduction in 2023, would resolve this gap by making reporting of these crimes to the CyberTipline mandatory.
- Clarifying requirement to report all CSAM-related activity – ESPs have differing interpretations of the scope of the present statutory requirement to report CSAM-related activity. The reporting statute (18 U.S.C. § 2258A) should be updated to clarify that ESPs are required to report to the CyberTipline any information relating to CSAM that they become aware of on their platforms, including apparent and imminent violations.
- Expand ESPs' retention period for CyberTipline report information – currently ESPs must retain information relating to CyberTipline reports for only 90 days. This time period is not sufficient to accommodate the volume of reports and law enforcement's investigative process and should be expanded. The REPORT Act (S. 474) would resolve this issue by extending the retention period from 90 days to 1 year.
- ESP reporting transparency – currently there is no recommended or required structure for ESPs to issue transparency information relating to their reporting to the CyberTipline. Transparency requirements relating to CyberTipline reporting would provide Congress and the general public with substantive information relating to online platforms' efforts to make their sites safer for children and also would drive development of best practices. The EARN IT Act, which is pending re-introduction, would provide a framework for the preparation and issuance of ESP transparency reporting.
- Introduce measures to incentive reporting and removal of child sexual abuse material – currently child victims have no recourse when a company knowingly facilitates the online distribution of sexually explicit imagery in which they are depicted or fails to respond to a notification that such imagery is circulating on their platform. The immunity provided to companies under the Communications Decency Act (47 U.S.C. § 230) denies child victims and their families of their day in court when an online platform is involved in their sexual exploitation. The EARN IT Act, which is pending re-introduction, would revise the Communications Decency Act to provide child victims with a private right of action when an ESP knowingly hosts or facilitates the distribution of sexually abusive material in which the child is depicted or refuses to remove such material after receipt of a notice.