TESTIMONY OF
CEO John Pizzuro, Raven
Commander, New Jersey Internet Crimes Against Children (Ret)
New Jersey State Police (Ret)

for the

UNITED STATES SENATE JUDICIARY
SUBCOMMITTEE ON CRIME AND COUNTERTERRORISM
Ending the Scourge: The Need for the STOP CSAM Act

March 11, 2025

Chairman Hawley, Ranking Member Durbin, and distinguished members of the Senate Judiciary Subcommittee on Crime and Counterterrorism, thank you for the opportunity to testify today on the need for the STOP CSAM Act. There is no more pressing issue than safeguarding our children and helping those who are on the frontlines to protect our children. That is why Raven was created, with the singular mission to "Transform the Nation's Response to Child Exploitation."

Members of Raven carry out the mission in a few important ways. Raven meets with members like you to discuss the real-life cases our law enforcement officers see every day. We explain the trends, the technology needs, and the achievements and the challenges of those working tirelessly to fight evil. We draft and review legislation regularly, providing input on how to best tackle the various issues within child exploitation. Finally, we advocate vigorously for more funding for our nation's overwhelmed and understaffed law enforcement and the task forces that support them and ultimately keep our kids safe.

I am retired from the New Jersey State Police, where I served for twenty-five years, seven of which were as the Commander of the New Jersey Internet Crimes Against Children (ICAC) Task Force. Raven has over 100 years of combined law enforcement experience. We have seven additional retired ICAC Commanders and a prosecutor with 20 years of experience in bringing justice to victims and their families. **We have thoroughly reviewed the STOP CSAM ACT and applaud its introduction.**

I want to highlight several aspects of the bill that if signed into law, would improve investigative outcomes for law enforcement and provide protection and justice for victims of child sexual abuse.

SECTION 2 – PROTECTING CHILD VICTIMS AND WITNESSES IN FEDERAL COURT

This section amends the statute to clarify that some of the protections for child victims follow them into adulthood. Many child victims of sexual abuse and CSAM do not report

their abuse until they are adults, and the changes in this bill provides them the support they need and deserve. Walking into a courtroom to testify on any topic is intimidating to most people. Now, imagine having to do that in front of your abuser as someone who has suffered unimaginable crimes at their hands. Survivors and victims deserve our best protections.

They also deserve privacy. Since co-founding Raven, I have talked with CSAM survivors whose personal information was exposed through discovery in criminal and civil cases. Their online abusers were then able to find this information and use it to traumatize the victims all over again. Simply redacting their names is oftentimes not enough to protect them. STOP CSAM defines their protected information to include their name, address, phone number, online username, and *any* information that either alone or in combination with other information could lead to the disclosure of their identity. This language will protect them from being further victimized for their entire life. STOP CSAM also gives these privacy protections teeth by providing the court with a remedy to ensure all parties comply with the law.

SECTION 4 – CYBERTIPLINE IMPROVEMENTS, ACCOUNTABILITY AND TRANSPARENCY BY THE TECH INDUSTRY

The law currently requires electronic service providers who detect an *apparent* violation of certain crimes that involve child sexual abuse material to make a report to the National Center for Missing and Exploited Children (NCMEC). The revised language requires providers to report *apparent*, ***planned and imminent*** violations. Platforms often detect grooming behavior or other signs of a child in distress, but they have total discretion to decide whether or not to report information about planned or imminent offenses. This revised language will undoubtedly result in saving children from abuse before it happens. As a former ICAC Commander, I can say that our best day is when we can rescue a child before they are abused.

The CyberTipline statute requires tech platforms to send a report to NCMEC when they are aware of a specified violation. But the only information that must be contained in the CyberTip is the provider's contact information. That's it. Providers can, in their sole discretion, include information about the "facts and circumstances" of the apparent violation. There is no required information or uniformity. You've heard the statement; "garbage in – garbage out." In many instances that is what we get. Some providers even submit blank reports—which is all they currently need to do to comply with their legal obligations.

These platforms often possess a lot of information on a particular offender or account, and they simply choose not to report it to NCMEC. This lack of detailed reporting impedes the work of law enforcement as it is often impossible to act on and begin an investigation. We

can no longer trust big tech to submit what is needed, when so many do the bare minimum required.

The STOP CSAM Act changes that and would require providers to submit limited additional data in its reports to NCMEC. Data such as the name, address, email address, account identifier, and IP address of the individual who is a subject of the report. They would be required to include any CSAM that is the subject of the report if that CSAM was detected on a publicly available area of their platform. Additionally, they would be required to indicate whether the reported CSAM has been the subject of another report or is the subject of multiple contemporaneous reports due to widespread distribution.

These added requirements will provide law enforcement with much more information than they are currently receiving and will result in the quicker prioritization of leads, actionable investigations and more arrests and prosecutions.

The STOP CSAM Act requires that these reports are made to the National Center as soon as reasonably possible, but not later than 60 days after obtaining such knowledge. Providers have never had a deadline and oftentimes submit reports months after the violation takes place. This delay results in information too stale for law enforcement to act upon.

SECTION 5 – EXPANDING CIVIL REMEDIES FOR VICTIMS OF ONLINE CHILD SEXUAL EXPLOITATION

Seeking justice for victims and punishment for the guilty is what law enforcement officers in this country do every day. Through the experience of handling thousands of child exploitation case, it is abundantly clear that social media and other online platforms play a much bigger role in the victimization of our youth than they will admit. The collection of "bad guys" sitting behind the phone or computer screen causing harm all use the same tool to commit their crimes: big tech. It is time to change the game and allow victims and survivors to seek a civil remedy when big tech knowingly contributes to their exploitation. Once big tech knows it will have to answer for their inactions in court, they will finally begin to take child safety seriously.

Should we let section 230 immunity continue to keep every victim and surviving family member from their day in court or do we provide a legal avenue for the most egregious and serious of cases to proceed? I want to highlight just one of the cases where the new 2255A provision in STOP CSAM could make a difference.

You have likely heard of the John Doe #1 and John Doe #2 v. Twitter case. This horrific chain of events began back in 2017 when two young boys were solicited on Snapchat at the age of 13 to send sexually explicit images to someone they believed was a 16-year-old female classmate. As is often the case, the "16-year-old girl" was really a bad actor who

began extorting the boys for more images and videos under threat of exposing them to their friends and family.

The boys continued to send sexually explicit photos and videos out of fear. Eventually they were able to block the predator on Snapchat and the communication ended.

In 2019, the images and videos of John Doe #1 and #2 began to appear in a video compilation on Twitter. On December 25, 2019, Twitter was first notified of the video by a concerned citizen on their platform. That person provided thorough information in the reporting form about which accounts were posting and sharing the video. Twitter did nothing.

On January 19, 2020, the two boys, then 16 years old and in high school, first found out from classmates that their images were being distributed on Twitter. On January 21st John Doe #1 filed a complaint with Twitter requesting the video be removed. Twitter responded by email acknowledging receipt of his request and asked him to provide photo identification so they could verify his age and identity. He did that immediately.

John Doe #1 and his mother continued to make reports to Twitter when they did not receive a response or see any action to remove the video or the accounts distributing it. On January 28th – a week after John Doe provided his identification and age, Twitter replied stating that the video did not violate their policies.

John Doe's mother was able to contact a Homeland Security Agent who reached out to Twitter on January 30th and *that* is when they finally removed the video and suspect user accounts who had posted the content.

Twitter did not make a mandatory report to the National Center for Missing and Exploited Children throughout this entire reporting process by John Doe and his mother.

The sexual abuse images of those two boys remained on the Twitter platform for over a month with no action. Just one post had over 167,000 views and had been re-tweeted over 2,000 times.

Imagine how hopeless these boys and their parents felt then and must still feel today as they are still waiting for justice. They filed a lawsuit against Twitter over four years ago. Their complaint against Twitter was dismissed by the District Court, in part, due to section 230 immunity. Their latest appeal is pending before the 9th Circuit Court of Appeals today. I hope they win, but even if they do, that is one case in one part of the country. Section 230 would still stand as a defense in the next case. STOP CSAM would unlock the courtroom doors and remove section 230 as a barrier to cases like this one.

CONCLUSION

The STOP CSAM ACT is a comprehensive piece of legislation that will make a positive impact in child exploitation cases. It will improve the experience of victims as they navigate the courtroom setting. It will protect and preserve their privacy far beyond the conclusion of their cases. It will improve the information law enforcement receives from a CyberTip, allowing for more successful investigations and prosecutions. Finally, it will provide a long-overdue civil remedy for so many survivors who have been further victimized by big tech. **Raven urges you to pass the STOP CSAM ACT**.