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

for the

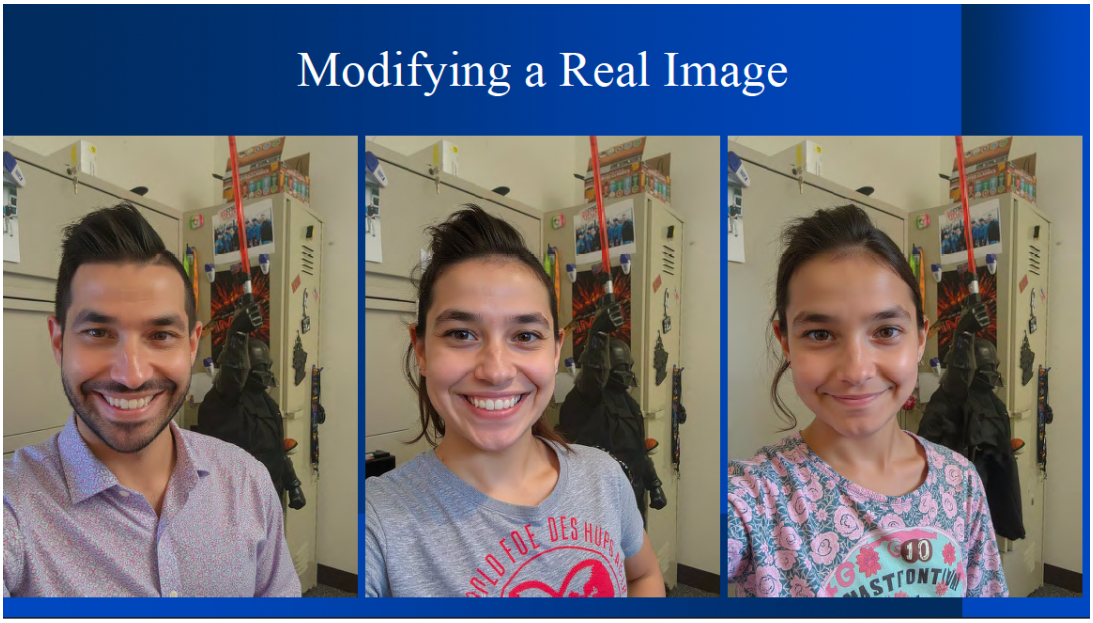
UNITED STATES SENATE JUDICIARY COMMITTEE
Children's safety in the Digital Era: Strengthening Protections and Addressing Legal Gaps
February 19, 2024

Chairman Grassley, Ranking Member Durbin, and distinguished members of the Senate Judiciary Committee thank you for the opportunity to testify today on Children's Safety in the Digital Era. For me, there is no more significant issue than safeguarding our children and helping those who are on the frontlines protect our children. So much so, that Raven was created with the singular mission to "Transform the Nations Response to Child Exploitation."

Sadly, this is the fourth time Raven has testified in Congress, yet very few pieces of Child Protection legislation have passed into law. I applaud the Senate Judiciary Committee for passing several pieces of legislation last Congress only to fall flat in the House despite our best efforts. In addition to the slow passage of laws, we must deal with the special interests groups like the tech lobby or other organizations that have a financial incentive that create a false narrative. I promise you the adversary of change are those who want the status-quo to protect their profits and interests. Our collective objective should be the protection of our children. We cannot let the perfect be the enemy of the good. That starts with legislation. We are failing to protect our children and failing those who protect them. Senators, I need your help. I need help from Congress and The Trump Administration. This problem must not exist any longer and we need every one of us to be part of the solution.

It was exactly two years ago when I testified before this Committee and since then new threats have emerged for our children when we have yet to address the old ones. Artificial Intelligence now allows offenders to groom children at mass and offenders do not even need to groom a child to have them send an image. Now, they can take a non-explicit image of a child that is easily accessible from the internet and turn that image into CSAM, using it for sextortion. ***(Exhibit 1)*** Historically, it always has been about offenders' sexual gratification but today there is now a financial component. Everyday our inaction to pass legislation results in children being victimized. As someone who has dedicated their life to protecting our children. I can assure you we need better awareness, support, policy and legislation to protect our children.

Exhibit 1



The sad reality is that our children have not been a priority, and I am here to ask that you make children our priority. Today our children live online and that is where they are at risk. Meanwhile, the Tech Industry has provided limited solutions to protect our children better. There has not been a decrease in online victimization only a substantial increase. The Tech industry's answer has been to reduce Trust and Safety teams, move to end-to-end encryption, and hide behind Virtual Private Networks (VPNs). Everything they do to protect children is "Voluntary" which includes the information that they share with NCMEC and law enforcement. The truth is that that they do the bare minimum of what is required. While there are committed trust and safety individuals within tech companies, their corporate structure and mission is an impediment to any progress those dedicated trust and safety persons can advance. "If a tech company does not see a problem, then they can't be responsible for the problem." It is that pervasive thinking that has led us to where we are. We fight today against the biggest lobby. Many times, I am in one waiting room and the Tech Lobby is in the other. In 2023, there were 36 million Cybertips yet only 250 came from Apple despite having over a 57% market share in the United States[1]

On January 31, 2024, Discord appeared in front of your committee and according to detectives that serve legal process on Discord (subpoenas) they notify users of the legal process served. By the time Law Enforcement hits the door with a court authorized Search Warrant the users devices are wiped erasing evidence of their wrongdoing along with the victims they have been victimized.

[1] https://gs.statcounter.com/vendor-market-share/mobile/united-states-of-america

If an offender's username gets identified and flagged and banned by an ESP, the associated screen names with the same IP Address are allowing the potential offender to simply use another screen name under the same IP Address. Furthermore, ESPs can see foreign IP Addresses that target our children for Sextortion, yet they are not identified and banned.

The risk comes from our online world. I wish I did not have to be here to testify on this issue because it would mean our children are safe when they go online. The truth is, we have not protected our children sufficiently due to the ever-increasing use of social media apps and the growth of their online lives. Their risk for harm has increased at such a significant pace that shielding them from abuse and exploitation has become untenable. To quote a sentiment shared by thousands of global experts in this space: "We cannot arrest our way out of this problem." Today there are countless victims of Child Sexual Abuse Material (CSAM), Child Trafficking, hands on offenses, Sextortion, and other exploitative crimes. The sad reality is that we are failing to protect our children from the threats they face online. We are also failing to equip law enforcement with legislation and resources to identify victims and identify offenders.

Those who would protect our youth are overburdened and under-resourced, which makes children vulnerable. Our nation's young people are unable to escape from the bombardment of posts, reels, and online social interaction. Artificial Intelligence and algorithms push children to those viewers who crave content and are interested in children. These same algorithms push harmful content to children. A major disadvantage of our global society is that any offender can reach any victim, anywhere in the world, through any app or gaming platform. With AI, offenders can now machine learn and mimic the behavior of children to infiltrate their lives allowing them to groom children at scale. We live in a world where everyday tasks increasingly are accomplished through apps, from shopping, to making a flight reservation, to – sadly - even children buying drugs.

I am here today as the CEO of Raven, an advocacy group comprised of 12 professionals, including seven retired Internet Crimes Against Children (ICAC) Task Force Commanders, who have committed their lives to the advocacy and protection of children. The Internet Crimes Against Children Task Force Program (ICAC program) helps state and local law enforcement agencies develop an effective response to technology-facilitated child sexual exploitation and Internet crimes against children. The ICAC program is a national network of 61 coordinated task forces, with at least one in each state, representing more than 5,400 federal, state, and local law enforcement and prosecutorial agencies. The ICAC Task Force was authorized by the Protect Our Children Act in 2008 at time when there was one computer per household and not the 17 Internet capable devices today. [2] The Protect our children act had an authorization of 60 million in 2008 which remains unchanged. The amount they get appropriated is 31.9 million which is just over 50% percent of their authorized amount. That is an average of $522,950 per task force. That funding goes directly to state and local law enforcement that is responsible for most of the child exploitation cases in the United States. How do you expect these men and woman to keep our children safe with that amount of funding? These agencies are engaged in both proactive and

[2] https://www.broadbandtvnews.com/2024/01/12/average-number-of-connected-devices-in-us-internet-households-reaches-17/

reactive investigations, forensic investigations, and criminal prosecutions. This ICAC program also encompasses training and technical assistance, victim services, and community education.[3]

I am retired from the New Jersey State Police, where I served as the Commander of the Internet Crimes Against Children task force from 2015 to 2021. I personally experienced the struggles of how best to protect our children online. We witnessed children targeted by offenders across all platforms – no social media or gaming platform was safe. Apps such as Snapchat, X, Kik, Telegram, Discord, LiveMe, and Meetme, to gaming platforms and online games such as Minecraft, Roblox, and Fortnite. These platforms represent just a fraction of the places where offenders regularly interact with children. If the platform allows individuals to chat, or a way to share photographs and videos, I assure you there is a very real danger that offenders are using that access to groom or sexually exploit minors. Sadly, in addition to sexual exploitation, the platforms allow children to buy drugs such as Fentanyl.[4]

Our children's world has become focused on likes, followers, and views, and in this way social media exploits vulnerabilities in our children's psychology. In an interview with Axios, the former President of Facebook stated, "That means that we needed to sort of give you a little dopamine hit every once in a while, because someone liked or commented on a photo or a post or whatever ... It's a social-validation feedback loop ... You're exploiting a vulnerability in human psychology ... [The inventors] understood this, consciously, and we did it anyway." [5]

That interview occurred on November 9, 2017 - more than seven years ago, and our dependence on technology has only increased. Cell phones have become ubiquitous, even in elementary schools, providing offenders with an entirely new way to exploit children on the playground. Victims have become younger and younger. Especially as children have access to smart phones at an earlier age. Children are made vulnerable on these platforms as the result of poor moderation, the absence of age or identity verification, and inadequate or missing safety mechanisms. Of course, as the amount of screentime has increased, so has the likelihood the children can be groomed and manipulated.

Grooming is defined as simply manipulating and gaining a child's trust, but it is much more than that. Grooming is what offenders do to victimize children, and it happens daily to unsusceptible children who cannot see the danger. Children do not know the threat online because they primarily engage in their online world in a safe place. As a result, the amygdala, the fear center of their brain, is not activated, and children do not see the danger. This is what offenders will

---

[3] The ICAC Task Force program was developed in 1998 response to the increasing number of children and teenagers using the Internet, the proliferation of child sexual abuse images available electronically, and heightened online activity by predators seeking unsupervised contact with potential underage victims. The Providing Resources, Officers, and Technology to Eradicate Cyber Threats to Our Children Act ("the PROTECT Act") of 2008, (P.L. 110-401, codified at 42 USC 17601, et seq.), authorized the ICAC program through FY 2013. On November 2, 2017, the Providing Resources, Officers, and Technology to Eradicate Cyber Threats to (PROTECT) Our Children Act of 2017 was signed into law, reauthorizing the ICAC Task Force Program through FY 2022. More information is available at https://www.icactaskforce.org/.

[4] https://ktla.com/news/local-news/mother-mourns-sons-death-from-fentanyl-laced-drugs-purchased-on-snapchat/.

[5] https://www.axios.com/2017/12/15/sean-parker-facebook-was-designed-to-exploit-human-vulnerability-1513306782

capitalize on. I typed, "how to do I exploit children" into Chat GPT and it would not answer so I changed my request slightly to "how children are groomed" and it gave me all I needed on how to groom children.

While sending compliments, virtual currency, gift cards, and other incentives are certainly part of grooming, today's offenders do even more to access children's trust. Offenders research children to know what they like, and do not like, what music they listen and so on. The offender will then mirror their words and repeat the exact language. The child will then see someone who is just like them. Chat forums on Tor share success stories on successfully grooming children of all ages. Each offender will attempt to groom hundreds of children using various techniques beyond just sending a picture or a video. We discuss numerous "in real life" dangers in school curriculums, yet online grooming is not part of it. With the advent of Artificial Intelligence, I can now simply machine learn someone's profile and groom children at mass. What do we like to talk about most? Ourselves. When wors are written our subconscious brain sees the repeated words and language that we use as "people that are similar to us" A.I will be able to do this through machine learning at mass. This type of Grooming can also help recruit extremists.

As the New Jersey ICAC Commander, I struggled with the significant increases in investigations, arrests, and victims we faced each year. The most staggering increase we faced was self-generated CSAM cases – children taking sexual images of themselves as the request of offenders. These were not images of older teens sending photos of themselves to their boyfriends and girlfriends – we began to see images of 7, 8, and 9-year-olds in sexual poses. The online landscape is horrifying because offenders know this is where our children live, and they recognize there are not enough safeguards to keep them at bay.

During one case, I received a call from a Child Advocacy Center in another state. The advocate told me a mother had just arrived with her 8-year-old daughter after she found sexual abuse videos on the child's phone. An offender had obtained a sexually abusive video of an 11-year-old girl and then used that video to coerce approximately 60 children to share sexually explicit videos of themselves. This included a video of a 12-year-old girl abusing her 1½-year-old brother. These child victims were located throughout the United States and Canada and were using a popular live-streaming app. This is one example of thousands of cases throughout the United States and the globe.[6]

It is important to understand that the CyberTipline is challenging law enforcement not only with respect to the quantity of leads, but also the quality of leads. According to data from several ICAC Task Forces only approximately 5% of Cybertips received from NCMEC result in an arrest. This is not because of NCMEC, it is because of the quality of information they receive from the Electronic Service Providers. This has burdened ICAC and as a result they prioritize inefficient investigative leads due to the mandated prioritization of Cybertips. A solution would be the addition of discretionary language in the updated version of The Protect Our Children Act that would give the same qualified immunity bestowed to NCMEC and Tech Industry to Law

[6] https://www.app.com/story/news/crime/2019/09/24/lakewood-sex-offender-had-more-than-1-000-images-child-porn-his-iphone-feds-say/2435710001/.

Enforcement so they can go after the most egregious offenders and allocate their limited resources more effectively.

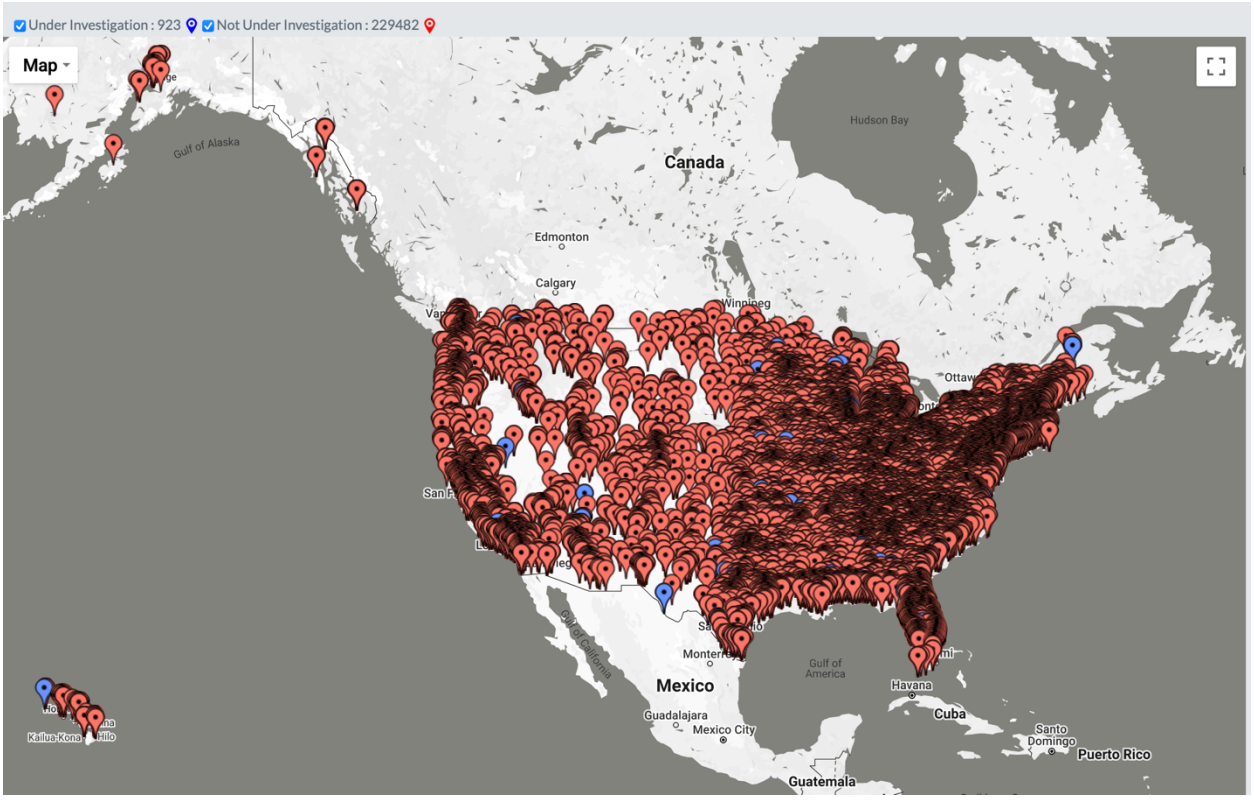
Most of the investigative leads provided by service providers, through NCMEC, to the ICAC Task Forces are not actionable, meaning they do not contain sufficient information to permit an investigation to begin. The lack of uniformity in what is reported by service providers results in law enforcement being forced to sort through thousands of leads trying desperately to identify worth-while cases. Cases where abusers and offenders who are considered particularly sadistic and dangerous. The *Ackerman* case out of the 10th Circuit, and the *Wilson* case out of the Ninth Circuit, have also increased the burden on law enforcement officers trying to review CyberTips.

As noted above, the sheer volume of Cybertips also prevents law enforcement from pursuing proactive investigative effort that would efficiently target the most egregious offenders. For example, peer-to-peer file sharing investigations and operations used to allow ICAC Task Forces to efficiently locate and apprehend hands-on offenders.[7] In the last 90 days, alone, there have been 229,482 IP addresses throughout the United States that have distributed known CSAM images and videos through peer-to-peer networks. Yet only 923 - less than 1% - are being investigated **(see Exhibit 2).** Consistently, 75% of these cases have resulted in successful prosecutions. Significantly, the most rigorous studies involving interviews with offenders have shown that between 57% and 85% of individuals arrested for these crimes have committed undetected sexual abuse of minors; on average, those offenders have assaulted between 10 to 13 victims.[8] Due to the overwhelming volume of Cybertips, law enforcement is simply not investigating peer-to-peer to the degree that it wants and should.

EXHIBIT 2

[7] https://www.nj.gov/njsp/news/2016/20160818.shtml

[8] https://www.ojp.gov/ncjrs/virtual-library/abstracts/butner-study-redux-report-incidence-hands-child-victimization-child.



ICAC Task Forces throughout the United States used to regularly conduct undercover operations targeting offenders who traveled to meet and assault individuals they believed were 10- to 14-year-olds. All of these undercover investigations are performed using social media apps or online ads that solicit the sexual assault of children. When arrests are made, investigators rarely find it is the first time the offender has traveled to sexually abuse a child.

These offenders bring drugs, alcohol, sex toys, and other paraphernalia. In one case an offender brought a dog leash and collar so he could be "walked" by a 12-year-old.[9] Task forces throughout the U.S. would conduct these operations on a routine basis, and they were very successful. The North Florida ICAC task force, for example, conducted 48 of these operations, arresting thousands of individuals, and obtained a conviction rate of 98.7%. Unfortunately, task forces are no longer able to perform as many of these types of operations - they are resource intensive, and the volume of reactive cases prohibits it.

The Darknet, including Tor, has become the newest online haven for child exploitation.[10] Some forums and boards contain the most abusive child exploitation videos and images law enforcement has encountered. Chat forums allow offenders to create "best practices" on how to groom and abuse children effectively. A post named the "Art of Seduction" that explained how to "seduce" children was read more than 54,000 times. Other posts discuss the best way to introduce sexual activity to children without alarming them or offer such topics as "Thoughts on

[9] https://www.nj.gov/oag/newsreleases19/pr20190424a.html.

[10] The Dark Net is an encrypted portion of the internet that is not indexed by search engines where users can communicate anonymously without divulging identifying information, such as a user's location. Tor is one network on the Dark Net.

having oral sex with 0-2-year-olds." ***(See Exhibit 3).*** These conversations are horrific, yet Tor is easily downloaded as a web browser, and children and teens can install it on their phones and begin accessing it within minutes. It is estimated that 12% of Tor users come from the United States and all anyone has to do is go to the App store to download the App to their Apple or Android device.

EXHIBIT 3

Pages: [1] 2 3 4 ... 30

NEW TOPIC NEW POLL NOTIFY MARK READ

SUBJECT / STARTED BY	REPLIES / VIEWS	LAST POST
Guidelines and Staying Safe new Started by GLover	9 Replies 58,859 Views	06 July, 2020, 10:37:54 by thewhiteknights
Pedomom: Thinking about my daughter having sex arouses me totally new Started by annione « 1 2 3 »	38 Replies 40,261 Views	Today at 17:29:39 by Oberon
Underage Kids and Orgasms new Started by dantexvergil « 1 2 3 »	30 Replies 23,944 Views	Today at 07:10:02 by littleboylost
confused mom new Started by anna34 « 1 2 »	15 Replies 5,462 Views	08 May, 2022, 21:58:30 by anna34
With whom did you make Pedo experiences? new Started by Pedomum « 1 2 3 »	30 Replies 20,552 Views	07 May, 2022, 19:44:54 by RogerTheShrubber
Masturbating around children new Started by Enchantress « 1 2 3 »	37 Replies 22,129 Views	25 April, 2022, 17:00:08 by smynevem
How to stop with those less than legal age? new Started by Robotboy	5 Replies 1,378 Views	24 April, 2022, 03:42:03 by LGlovie127
new kids new Started by gobu	11 Replies 3,081 Views	23 April, 2022, 13:06:58 by SecondChance
Baby sitting a friend's 9 year old daughter twice a week new Started by Exister « 1 2 »	29 Replies 11,972 Views	20 April, 2022, 22:05:16 by LGlovie127
Thoughts on oral sex with kids 0-2? new Started by TenderFlame2 « 1 2 3 4 »	50 Replies 31,591 Views	19 April, 2022, 12:03:11 by SecondChance

In one undercover operation a registered sex offender paid to sexually abuse an 11-year-old, spoke about how he was able to victimize his two-year-old nephew, and described how he groomed children into providing him with child sexual abuse videos. [11] The offender sent screen shots of his texts with children with whom he had connected using Kik, which revealed his technique for convincing them to send him sexually explicit material. He admitted sexually assaulting a massage therapist and indicated he wanted to kidnap an eight-year-old child, but he was afraid of being caught.

The individuals arrested by the New Jersey ICAC Task force on the Darknet paid to sexually assault and traffic children. These children were young as 3 years old. The offenders traveled to New Jersey from the UK, Germany, Canada and all throughout the United States. In my experience offenders will be hands on offenders. They are on Tor, to be anonymous, so they can find and victimize children. The only thing that stops them from being a hands-on-offender is the likelihood of being caught. One offender referred to himself as a category 3 pedophile, meaning he would only act against a child if the opportunity presented itself with likelihood of not being caught.

[11] https://www.justice.gov/usao-edca/pr/sacramento-county-man-sentenced-25-years-prison-sexual-exploitation-child.

Another offender, a Jersey City police officer, used the Wikr and Kik apps to communicate with his victims. He used those apps to communicate with undercover investigators, where he attempted to pay to sexually assault an 8- and 10-year-old girl. He then traveled to Atlantic City with condoms and cash, with the intent of abusing the child. These are just a few examples of the depravity that law enforcement deals with daily. The crimes that lead to their apprehension is nearly always only the tip of the iceberg – there is never just one victim.

The details of these undercover investigations shock the conscious. There is no shortage of case reports describing the sexual abuse of 11-year-olds. Or a mother who is targeted by an offender because her 5-year-old is too young to text but is of the age interest for the offender. Or the offender who brought a stuffed animal for the 10-year-old he was going to rape, along with a bottle of Viagra and other sexual devices for when the Viagra failed.

The impact of these cases does not only affect our children, but the law enforcement community as well. Investigators, prosecutors, child advocacy professionals, and everyone involved in these horrendous acts must bear witness to the depraved images, sounds, words, videos, and case specifics eroding their mental health. The toll these cases place on law enforcement's mental state comes with a price. We need to support these law enforcement professionals from a wellness standpoint. Many times, our law enforcement professionals suffer in silence with limited resources. Every day I would come to work and worry about the damage these cases do to the people investigating them. I am concerned about the lack of resources available to the law enforcement community from a wellness standpoint. No one can prepare you for what you see in these cases; once you see them, they are challenging to unsee. These cases will stay with investigators throughout their lives to the detriment of their lives and families.

I love this Country. It does not matter your party, your race, creed, or sexual preference we must protect our children. They are our most valuable resource. Their victimization will have a lasting impact on our nation. Every child deserves a world without their exploitation and in my experience, we have collectively failed to protect them and support those who protect them. If there is ever a time it is now. I understand the collective challenges our country faces and there are many issues that need attention, advocacy and resources. Despite these challenges I want nothing other to protect our children and those who protect them. We lose children to suicide, and sexual exploitation and those who protect them to burnout.

One simply can look at the statistics to determine the real story - what is truly happening to our children. I and my fellow members of Raven will meet with anyone whether its members of the Senate, House, The Trump administration, or Big Tech. Not to debate, not to cast blame but to honestly to come up with solutions to protect our children. Sadly, our experience has fell short of any legislation becoming law.

Based on what I have experienced and have seen, I can confidently tell you three things: At the moment the offenders are winning, our children are being exploited and victimized and those who are fiercely committed to protecting them are drowning and burning out. We need to get them the legislation and resources they need to protect our children. The solution is in your hands. I greatly appreciate everyone in this Committee staff and members that have shown the passion and interest to protect our children it gives me hope.

LEGISLATIVE SOLUTIONS:

- At the very least we must pass THE PROTECT OUR CHILDREN ACT and appropriate the full 70 million of the authorized amounts which still only brings it to approximately $1,147,540 per task force.
- Pass legislation that will require better reporting requirements from ESP's which would include data uniformity as seen in elements of STOP CSAM to increase the efficiency of Cybertips.
- Currently GAI is being prosecuted under the federal obscenity statute, however it does not require that the offender register as a "Sex Offender". There also needs to be enhanced penalties for using AI to groom children at scale.
- Open AI has many benefits, but it eliminates the guardrails put in place by some closed AI applications for child exploitation and other illegal uses. This should result in tougher criminal penalties for those who use open AI in an illegal manner.
- Pass the TARGETING CHILD PREDATORS Act that would prevent tech companies from disclosing law enforcement legal process requests for subpoenas for 90 days.
- Pass legislation that bans the tech companies from using algorithms to expose children to illegal and exploitative content.
- Device Based Age Identification which would prevent minors from downloading and creating online profiles that do not match their legal age.
- Using AI or identifying payment systems that could help flag financial transactions consistent with sextortion scams especially considering that they are transmitted from foreign IP addresses.
- Pass the SHIELD Act, which makes it a crime to knowingly mail or distribute an intimate visual depiction of an individual with knowledge of the individual's lack of consent, where what is depicted was not voluntarily exposed by the individual in a public or commercial setting, and where what is depicted is not a matter of public concern; or a visual depiction of a nude minor with the intent to abuse, humiliate, harass, or degrade the minor or to arouse or gratify the sexual desire of any person.
- Hold accountable those who are responsible for the proliferation of nonconsensual sexually explicit "Deepfake images and Videos" in the DEFIANCE ACT.