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

for the

UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY
Protecting Our Children Online

February 14, 2023

Chairman Durbin, Ranking Member Graham, and distinguished Senators, thank you for the opportunity to testify today on Protecting Our Children Online. For me, there is no more significant issue than safeguarding our children, as well as those who protect them from harm.

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), sextortion, and other exploitative crimes. The sad reality is that we are failing to protect our children from the threats they face online.

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. 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. 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 14 professionals, including nine 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 4,700 federal, state, and local law enforcement and prosecutorial agencies. These agencies are engaged in both proactive and reactive investigations, forensic investigations, and criminal prosecutions. This ICAC program also encompasses training and technical assistance, victim services, and community education.[1]

[1] 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,

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, from apps such as Snapchat, Twitter, Kik, Telegram, Discord, LiveMe, and Meetme, to gaming platforms and online games such as Minecraft, Roblox, and Fortnite. And these 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.[2]

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." [3]

That interview occurred on November 9, 2017 - more than five 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. 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 capitalize on.

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 then will see someone who

---

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/.

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

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

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.

As the New Jersey ICAC Commander, I struggled with the significant increases in investigations, arrests, and victims we faced each year. For example, in 2015 we received 2,315 Cybertips and made 125 arrests, and by the end of 2019 we had 8,000 Cybertips and we made 420 arrests. We understood the importance of trying to keep up, but even creative attempts to "do more with less" became unsustainable. And this was prior to COVID, when screentime increased substantially and cemented our children's reliance on apps. These challenges were frustratingly present with every ICAC task force across the United States. 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 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.[4]

The Protect Our Children Act of 2008 created a funding mechanism for Internet Crimes Against Children task forces that are responsible for 90% of the child exploitation investigations in the United States. But things have changed in this space since 2008. In 2008 there was an average of one computer per household. Today, families in the U.S. have an average of 20 Internet-capable devices, including phones, tablets, laptops, and gaming consoles. And the volume of data investigators must comb through to find victims has increased significantly. Reactive investigations take place when law enforcement receives information, such as a CyberTip, that a crime has occurred. A proactive investigation involves the use of intelligence to try to identify potential offenders.

Today, law enforcement is often unable to proactively investigate child exploitation cases due to the volume of Cybertips. As a result of the exponential increase in Cybertips (these tips increased by 2,800% between 2012 and 2021) law enforcement agencies have been forced to become

[4] 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/.

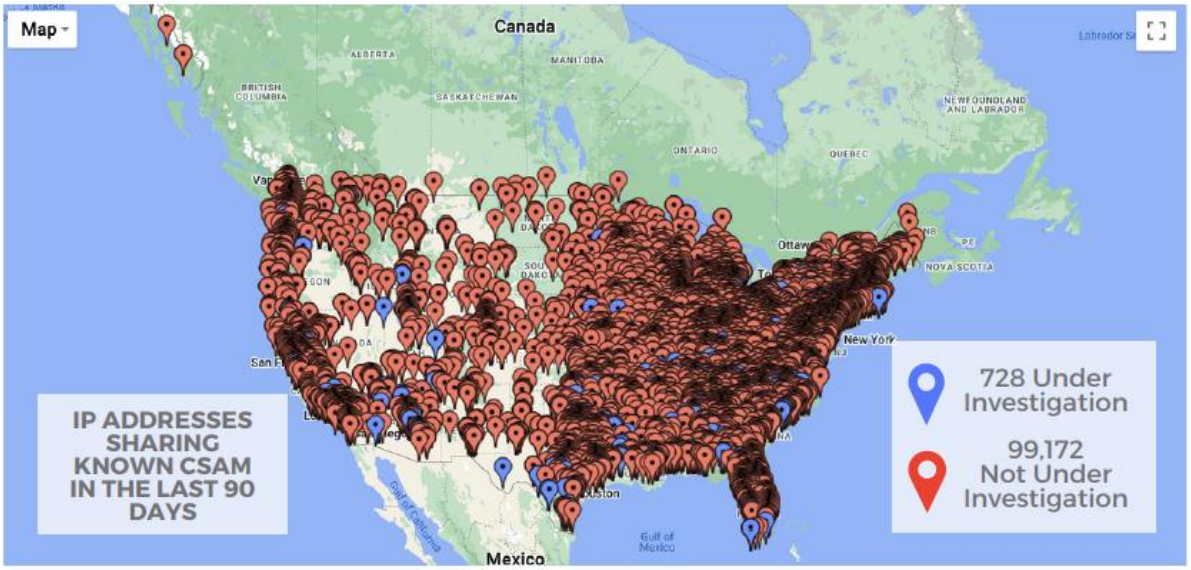
reactive, and most can no longer engage in the proactive operations that are designed to target the most dangerous offenders.[5]

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. 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 Fourth 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.[6] In the last 90 days, alone, there have been 99,172 IP addresses throughout the United States that have distributed known CSAM images and videos through peer-to-peer networks. Yet only 782 - less than 1% - are being investigated (see Exhibit 1). 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.[7] 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 1

[5] Reactive investigations take place when law enforcement receives information, such as a CyberTip, that a crime has occurred. A proactive investigation involves the use of intelligence to try to identify potential offenders.
[6] https://www.nj.gov/njsp/news/2016/20160818.shtml
[7] 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 an offender brought a dog leash and collar so he could be "walked" by a 12-year-old.[8] 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 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.[9] 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 having oral sex with 0-2-year-olds." 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.

---

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

[9] 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.

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. [10] 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.

Another offender, a Jersey City police officer, used the Wikr and Kik apps to communicate with his victims. He used those apps to communicate 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. They impact the law enforcement community. 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 every day. 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.

The reality is everything happens online. Offenders, including registered sex offenders, are lurking in the same places where our children are communicating with their friends or playing online games. There is very little to stop these predators from communicating with, and then grooming, any child they perceive as vulnerable. Those who seek to police these spaces are in need of significant help if they are to bring about change.

This past summer, I took a short walk on the beach in Point Pleasant. It was a beautiful 80-degree day, and along my half-mile walk I counted 67 children and teens on their phones, 12 of whom were making a TikTok video. I then came across a four-year-old who was lost and could not find his parent. Statistically, at least 1/4 of those children will be victimized. We are at a point where we need to identify what works and provide authorities with sufficient resources to

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

increase their protective capabilities. Children need our help. Every day, social media companies write posts and release one press release after another in which they tout their successes at keeping children safe. While appreciated, these actions constitute mere drops in the bucket. One simply can look at the statistics to determine the real story - what is truly happening to our children. Based on what I have experienced, I can confidently tell you three things: At the moment the predators are winning, our children are not safe, and those who are fiercely committed to protecting them are drowning and will continue to so unless we can get them the resources they need.