

S. HRG. 119–137

CHILDREN'S SAFETY IN THE DIGITAL ERA: STRENGTHENING PROTECTIONS AND ADDRESSING LEGAL GAPS

HEARING BEFORE THE COMMITTEE ON THE JUDICIARY UNITED STATES SENATE ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

FEBRUARY 19, 2025

Serial No. J-119-5

Printed for the use of the Committee on the Judiciary



www.judiciary.senate.gov
www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

61–324

WASHINGTON : 2026

COMMITTEE ON THE JUDICIARY

CHARLES E. GRASSLEY, Iowa, *Chairman*

LINDSEY O. GRAHAM, South Carolina	RICHARD J. DURBIN, Illinois,
JOHN CORNYN, Texas	<i>Ranking Member</i>
MICHAEL S. LEE, Utah	SHELDON WHITEHOUSE, Rhode Island
TED CRUZ, Texas	AMY KLOBUCHAR, Minnesota
JOSH HAWLEY, Missouri	CHRISTOPHER A. COONS, Delaware
THOM TILLIS, North Carolina	RICHARD BLUMENTHAL, Connecticut
JOHN KENNEDY, Louisiana	MAZIE HIRONO, Hawaii
MARSHA BLACKBURN, Tennessee	CORY A. BOOKER, New Jersey
ERIC SCHMITT, Missouri	ALEX PADILLA, California
KATIE BOYD BRITT, Alabama	PETER WELCH, Vermont
ASHLEY MOODY, Florida	ADAM B. SCHIFF, California

KOLAN DAVIS, *Chief Counsel and Staff Director*

JOE ZOGBY, *Democratic Chief Counsel and Staff Director*

CONTENTS

OPENING STATEMENTS

	Page
Grassley, Hon. Charles E.	1
Durbin, Hon. Richard J.	2
Blackburn, Hon. Marsha	4
Klobuchar, Hon. Amy	5

WITNESSES

Balkam, Stephen	14
Prepared statement	39
Responses to written questions	49
Goldberg, Carrie	9
Prepared statement	51
Responses to written questions	98
Guffey, Hon. Brandon	7
Prepared statement	100
Responses to written questions	103
Leary, Mary Graw	11
Prepared statement	104
Responses to written questions	124
Pizzuro, John	13
Prepared statement	131
Responses to written questions	141

APPENDIX

Items submitted for the record	143
--------------------------------------	-----

CHILDREN'S SAFETY IN THE DIGITAL ERA: STRENGTHENING PROTECTIONS AND ADDRESSING LEGAL GAPS

WEDNESDAY, FEBRUARY 19, 2025

UNITED STATES SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 10:17 a.m., in Room 226, Dirksen Senate Office Building, Hon. Charles E. Grassley, Chairman of the Committee, presiding.

Present: Senators Grassley [presiding], Cornyn, Lee, Hawley, Kennedy, Blackburn, Schmitt, Britt, Moody, Durbin, Whitehouse, Klobuchar, Hirono, Booker, Padilla, Welch, and Schiff.

OPENING STATEMENT OF HON. CHARLES E. GRASSLEY, A U.S. SENATOR FROM THE STATE OF IOWA

Chairman GRASSLEY. Good morning, everybody.

In today's digital era, our young people face risks that previous generations couldn't even have imagined. Even though technology brings amazing opportunities for education and growth, it also opens doors to new dangers that we must confront. This isn't the first hearing we've had on this issue, and, unfortunately, it probably won't be the last. We held a hearing on this same subject roughly a year ago when we brought CEOs from some of the largest social media companies to discuss safety issues on their platforms, and we held a similar hearing a year before that.

On the one hand, this is alarming because the problem is getting worse. In 2023, as an instance, the NCMEC Cyber Tip Line received 36-and-two-tenths million reports of suspected online child sexual exploitation, a 12 percent increase over 2022. And even though the numbers haven't been published for 2024, it seems that they're expected to go up.

Additionally alarming are the new technologies that are being used by bad actors to exploit children online. Predators can use generative AI, for instance, to take normal images of children and manipulate them to create novel forms of CSAM. In 2024 alone, NCMEC reported almost 61,000 instances of generative artificial intelligence CSAM.

Despite this, so far, Congress has enacted no significant legislation to address these dangers against children, and tech platforms have been unhelpful in our legislative efforts. Big Tech promises to collaborate, but they're noticeably silent in supporting legislation that would affect meaningful change. In fact, Big Tech's lobbyists

swarm this Hill, armed with red herrings and scare tactics, suggesting that it will somehow break the internet if we implement even these very modest reforms.

Meanwhile, these tech platforms generate revenues that dwarf the economies of most nations. So how do they make so much money? They do it by compromising our data and privacy and keeping our children's eyes glued to the screens through addictive algorithms. Indeed, in one recent study, 46 percent of teens reported that they're online, quote, "almost constantly," end quote. This has had severe mental consequences for adolescents. It has also led to a rise in sexual exploitation, as some algorithms have actually connected victims to their abusers.

Should such tech platforms be allowed to profit at the expense of our children's privacy, our children's safety, and our children's health? Should they be allowed to contribute to a toxic digital ecosystem without being held accountable? So I believe to everybody, the answer is very clear. When these platforms fail to implement adequate safety measures, they're complicit in the harms that follow, and they should be held accountable.

That said, there are some signs of encouragement. Just as new technologies are being developed that exacerbate harm to children online, so too are tech technologies being developed to combat exploitation. As one example, with AI, rapidly evolving open-source safety tools are being developed to recognize and report CSAM. Some of the witnesses here today will speak to the effectiveness of these tools.

Additionally, on a Committee with some of the most diverse viewpoints in the United States Senate, we have actually advanced bipartisan legislation that addresses legal gaps in our current framework, especially those related to the blanket immunity that Section 230 provides. Last Congress, for example, we reported several online safety bills out of Committee with overwhelming bipartisan support, and there are a number of bills that are being considered and refined this Congress, which we'll give attention to in due course.

That being said, we can't come up with a wise and effective legislative solution without first understanding the nature and scope of the problem. And so, that's why we're having this hearing today. Our witnesses come from various backgrounds and represent very diverse perspectives, all of which point to the need for our Committee to improve legislation and continue our work to keep kids safe.

So with that, I'll open things up to Ranking Member Durbin to give opening remarks. After that, we'll hear from Senators Blackburn and Klobuchar. Then, I'll introduce the witnesses and swear. Go ahead.

**OPENING STATEMENT OF HON. RICHARD J. DURBIN,
A U.S. SENATOR FROM THE STATE OF ILLINOIS**

Senator DURBIN. I want to personally thank you, Senator Grassley. This is unusual, a change in leadership in this Committee, and yet, an issue which we took up very seriously in the last few years on a bipartisan basis has survived the change. And in fact, this hearing is evidence of the determination of the Chairman. I'd like

to join him in that assurance that we're taking this issue very seriously.

It was almost exactly 2 years ago this Committee held a similar hearing. We heard from six witnesses about the harm social media does to our kids and grandkids: a mom whose son took his own life after he was bullied online; a young woman whose mental and physical health suffered as she chased the unattainable lifestyle depicted on Instagram and other apps; experts who told us how Big Tech designs their platforms to be addictive, keeping users online for longer and longer and longer times so they can be fed more targeted ads; individuals combating the tidal wave of child sexual abuse material, or CSAM, flowing across the internet.

At the end of that hearing, I told the witnesses and the many parents and young people in the audience I was going to roll up my sleeves, get to work, and pass legislation to protect kids from online safety concerns. That spring, the Committee reported five bills that help protect kids online, and included my STOP CSAM Act. And I want to thank Senator Hawley for joining me in that effort, which we hope to renew soon, along with bipartisan bills from Senators Graham, Blumenthal, Klobuchar, Cornyn, Blackburn, and Ossoff. These bills were reported out of this Committee unanimously.

For anyone who is a newcomer to Capitol Hill or to this Committee, you have the American political spectrum from one end to the other on this Committee. And for us to do anything unanimously is nothing short of a political miracle. We did it. The Senate Judiciary Committee contains Members across the spectrum, the most conservative Republican to the most progressive Democrat. It's almost unheard of to pass a bill unanimously, yet we did it—five times.

One of these bills, the REPORT Act, later signed into law by President Biden, strengthened the Cyber Tip Line, run by the National Center for Missing & Exploited Children. As for the rest, different story. Big Tech opened up a \$61.5 million lobbying war chest to make sure these bills never became law.

Now, let's be clear. None of these bills are the silver bullet that would make the internet completely safe for our kids. But they would be significant steps toward finally holding tech companies accountable for the harms that they caused, the damages they caused, the death that they caused, and that's why the tech companies opposed them as strongly as they did. They didn't do it publicly. Publicly, oh, it's such a great idea. But privately, they just beat the hell out of us.

So just over a year ago, I called in the CEOs of five major tech platforms—some I had to issue subpoenas—to demand answers on the record under oath. And that hearing produced some results. Several companies implemented child safety improvements just days before their CEOs came to testify. And Meta's CEO, Mark Zuckerberg, under pressure from Senator Hawley—artful questioning—gave a long-overdue apology to the parents his platform had hurt.

But apologies and too-little-too-late reforms are simply not enough. The dozens of parents and survivors in that room, the thousands impacted across the country demand more, and I for one

plan to follow through. In the coming weeks, Senator Hawley and I will reintroduce the STOP CSAM Act. This bill will finally open the courthouse door to families whose children have been victimized due to Big Tech's failure to safeguard their online platforms. I hope Senator Grassley will help me schedule a timely markup on that bill.

And this week, I'll join Senators Graham, Whitehouse, Hawley, Klobuchar, and Blackburn to introduce a bill to sunset Section 230 of the Communications Decency Act in 2 years. This is long overdue. Section 230 and the legal immunity it provides to Big Tech has been on the books since 1996, long before social media was part of our lives. To the extent this protection was ever needed, its usefulness for this so-called fledgling industry has long since passed.

I'm under no illusion that it'll be easy to pass legislation to protect kids online and finally make the tech industry legally accountable for the damage that they're causing. But they ought to face the same liability as every other industry in America.

Just last year, Big Tech and its allies in the House killed a bill, the Kids Online Safety and Privacy Act, a bill introduced, I believe, by Senator Blumenthal and Senator Blackburn, as well. That would have imposed a basic duty of care on tech platforms. It passed the Senate 91-to-3. But Big Tech did it in the House—couldn't even get it up for a vote.

The National Center for Missing & Exploited Children receives 100,000 reports to its Cyber Tip Line every single day. That's not just a statistic. Each of these reports involves a victim. It could be anything from images of a toddler being raped to a teenager being coerced, extorted, groomed, and encouraged to commit suicide—100,000 reports in the United States every single day. I hope everyone keeps that in mind as we hold this hearing. We cannot wait. We have to move. I hope it drives the public to demand Congress finally do something.

Chairman GRASSLEY. Senator Blackburn.

**OPENING STATEMENT OF HON. MARSHA BLACKBURN,
A U.S. SENATOR FROM THE STATE OF TENNESSEE**

Senator BLACKBURN. Thank you, Mr. Chairman.

And I want to say thank you to our witnesses for being here today. And, Mr. Guffey, we appreciate that you are here and sharing your story.

And, Mr. Chairman, you mentioned that it was over a year ago that we had tech execs in front of us and that nothing much has changed. That is the tragic part of this situation, that nothing much has changed. There's been window dressing. There have been ads that have been run saying, look at us, look at what we're doing. But, unfortunately, there is no enforcement to this.

That is why it is still dangerous for kids to be online. They're still facing online threats, exposure, sexual exploitation, drug trafficking, promotion of suicide, eating disorders. And the thing that is so interesting is, in the physical world, there are laws against this. It is only in the virtual space that it remains the Wild West and our children can be attacked every single day, nonstop, 24/7, 365. It is long overdue.

And the Kids Online Safety Act that Senator Blumenthal and I have worked on for years now has been mentioned already this morning. And there is such a broad bipartisan coalition, whether it's parents, principals, teachers, pediatricians, child psychologists, even teens themselves have come to us and have said, something needs to be done about this. We have had companies like Microsoft, X, Snap, who have supported this bill. Unfortunately, kids are still being harmed online. I talked to a mom recently whose child died. They met somebody online who sold them supposedly a Xanax. They met him on Snap. They took what they thought was a Xanax and they died. It was fentanyl.

So these are the dangers that are there. And while there is broad bipartisan support, Senator Grassley mentioned the lobbying efforts of some of the Big Tech firms and how they went with distortions and lies to the House, and this bill did not get through. So it is time to stop—stop this and get it passed.

Now, Senator Durbin mentioned the bills we sent out of Committee here last year. There was one that got signed into law, and it was the bill that Senator Ossoff and I did, the REPORT Act. And this deals with NCMEC's Cyber Tip Line and increases the time that evidence submitted to NCMEC has to be preserved, and it gives law enforcement more time to investigate, to get these criminals into court, and then get them locked up. And we still have so much work to do.

Now, Senator Klobuchar and I are going to lead the Privacy, Technology, and the Law Subcommittee, and these issues will be coming before us. We've got plenty of work to do. We're looking forward, Mr. Chairman—I look forward to convening this Committee, working to make certain that we are pushing this legislation, that we are going to protect our children in the virtual space.

Thank you, Mr. Chairman.

Chairman GRASSLEY. Senator Klobuchar.

**OPENING STATEMENT OF HON. AMY KLOBUCHAR,
A U.S. SENATOR FROM THE STATE OF MINNESOTA**

Senator KLOBUCHAR. Well, thank you so much, Mr. Chairman, and I am truly looking forward to working with Senator Blackburn on this important Subcommittee. As many of you know, Senator Lee and I chaired the Antitrust Subcommittee for a long time, but I actually think this situation right now, with the possibility of moving on these bills, is going to be a very positive development.

As Senator Blackburn just pointed out, despite the strong support that we have had from Senator Durbin and Senator Grassley—and Senator Graham when he chaired this Committee or was the Ranking on this Committee—we've just continued to run into roadblocks to passing these laws, and it's getting absolutely absurd. Senator Grassley is well aware of the antitrust tech bill that he and I lead that hundreds and hundreds of millions of dollars were spent against it in TV ads. And despite the fact that the companies—FANG, as we call them—have agreed in other countries to some of these consumer protections, that did not happen in America.

And I think that this piece of it, whether it's Instagram's promotion of content that encourages eating disorders, the frightening

rise of nonconsensual AI-generated pornographic deepfakes, or the tragic stories of kids losing their lives to fentanyl-laced pills will most likely be leading the way as we continue to push our antitrust and privacy and news bills.

Just this month, this Committee heard from Bridgette Norring of Hastings, Minnesota. Her son, Devin, was struggling with migraines and bought what he thought was a Percocet over Snapchat to deal with the pain. But it really wasn't a Percocet. It was a fake pill laced with fentanyl. And with that one pill—as we say, one pill kills—he died at age 19.

For too long, the companies have turned a blind eye when young children joined their platforms, used algorithms that pushed harmful content—they have done that—and provided a venue for dealers to sell deadly drugs like fentanyl. We know that social media also increases the risk of mental illness, addiction, exploitation, and even suicide among kids. I will never forget the testimony of the FBI Director telling us that, in just 1 year—I believe it was 2023—over 20 kids had committed suicide just because of the pornography and the images that had been put out there when they were innocently sending a picture to who they thought was a girlfriend or a boyfriend.

That's why this Committee has taken this on on a bipartisan basis, and I am hopeful that this hearing will be the beginning of actually passing these bills into law.

Representative Guffey, you and I met through Senator Cruz, and the bill that he and I have, the TAKE IT DOWN Act. We have an additional bill that Senator Cornyn and I have that's really important that's passed through this Committee, the SHIELD Act. And as you know all too well, the threat of dissemination alone can be tragic, especially for kids.

We need to enact the Kids Online Safety Act, which, thanks to Senators Blumenthal and Blackburn, have passed the Senate on a 91-to-3 vote. As we know, some of these are stalled out in the House. We need to get the Federal rules of the road in place for safeguarding our data. According to a recent study, social media platforms generate \$11 billion in revenue in 2022 from advertising directed at kids and teenagers—including \$2 billion in ad profits derived from users age 12 and under.

I am supportive, as was mentioned by Senator Durbin, of the legislation that he and Senators Graham and Hawley and many others to open the courtroom doors to those harmed by social media by making those reforms to Section 230. That legislation was enacted long before any of this was going on. And somehow, with respect to other industries, we've been able to make smart decisions to put more safety rules in place. Just ask those passengers that were on that flight that flipped upside down in Toronto who were in those seats that were the result of safety rules that were put in place.

And yet, when it comes to this, we just put up our hands and say, no, they're lobbying against us, or they have too many, or we like some of the people that work there—and we do nothing. And by doing nothing, instead of reaching some reasonable accommodations of settlements or things we can do on legislation, we just let them run wild at the expense of our kids' lives.

Thank you.

Chairman GRASSLEY. When you consider five bills got out of this Committee last Congress, and over the last few years, Congress has only been in session about 2½ days a week—it's supposed to be a new regime. I'm not sure that it is. And I would hope that some of you folks on the Democrat side would push Republicans to make sure we keep the Senate in session more than 2½ days a week so we can get some of this done because we had hardly any important legislation in the last 2 years. We were basically just a confirming body. Take that. I hope you enjoyed doing that like I enjoyed complaining because we were only meeting 2½ days a week when the Democrats controlled the Senate.

I'm going to introduce our guests today. Our first witness, Mr. Brandon Guffey, you serve now in the South Carolina House of Representatives. Following the tragic loss of your son, Gavin, Mr. Guffey became an advocate for mental health awareness and combating online crimes. And as Senator Blackburn said, we're sorry for the loss of your son, Mr. Guffey. It's probably hard for you to be here to talk about it, but thank you for being here.

Next, we have Ms. Carrie Goldberg, a plaintiff's attorney and founder of the law firm C.A. Goldberg, PLLC. She specializes in representing victims of sexual abuse, child exploitation, online harassment, and other forms of digital abuse.

Professor Mary Leary, a former Federal prosecutor, current law professor at Catholic University of America. Professor Leary directs the law school's modern prosecution program, and her scholarship focuses on exploitation of women and children. Professor Leary has an upcoming article that dives deeply into the history of Section 230 and its role in facilitating child sexual abuse material.

Mr. John Pizzuro is CEO of Raven, started as a former law enforcement, Raven gathers subject matter experts across multiple disciplines to help protect children from online exploitation. Mr. Pizzuro is a former commander of the New Jersey Internet Crimes Against Children Task Force program.

Mr. Stephen Balkam, CEO and founder of Family Online Safety Institute. This international nonprofit is dedicated to making the internet safer for kids. Before founding the institute in 2007, Mr. Balkam spent 30 years as a leader in the nonprofit sector, championing online safety. His work at the institute brings together those in government, industry, and the nonprofit sector to create a culture of responsibility.

Now, I'd like to ask you to stand and be sworn. Raise your right hand.

[Witnesses are sworn in.]

Chairman GRASSLEY. They have all answered affirmatively.

Mr. Guffey, we'll start with you and go from my left to my right.

**STATEMENT OF HON. BRANDON GUFFEY, FATHER,
AND REPRESENTATIVE, SOUTH CAROLINA HOUSE OF
REPRESENTATIVES, ROCK HILL, SOUTH CAROLINA**

Representative GUFFEY. Thank you, Mr. Chairman, distinguished Senators. Thank you for the opportunity to testify today. My name is Representative Brandon Guffey, and I'm here to share why pro-

tecting youth from online dangers and holding Big Tech companies responsible is now my life's mission.

Sometimes God sends you down a path that you never thought you would be on. In July of 2022, I lost my oldest son, Gavin Guffey, to suicide. On Gavin's last Instagram post a week prior to his death, he said, "This week, help me look up to where my head should have been years ago. Jesus, in His word, has given me a high that no other can compare to His love." He ended that post with a <3 sign. On July 27, Gavin would send out the <3 sign again on a black screen to his friends and his younger brother, Coen Guffey, who's with me here today. At 1:40 a.m., Gavin took his life.

We quickly learned that Gavin was contacted on Instagram around midnight when he told his friends he would jump off the game to chat with her. In just 1 hour and 40 minutes, my son was gone. The predator that contacted Gavin was recently extradited to the U.S. 2 weeks ago from Lagos, Nigeria.

The predator not only attacked my son, Gavin, who was 17, but also began to extort my 16-year-old son, my 14-year-old cousin, and then myself. One of the messages I received read, "Did I tell you that your son begged for his life?" I hope you ask, How is this possible? It's possible because Instagram removed the profile that attacked Gavin, but left up the additional profiles that predators use. One of those is the account that began to attack my family after Meta was fully aware of this predator.

I vowed from that moment that I would make it my life's mission to protect children online and would not stop. I was shortly elected to the South Carolina House, and within 4 months of taking office, successfully passed what is now known as Gavin's Law. Sextortion is mandated in education throughout the State of South Carolina, and every kid at least has to have some awareness so they don't feel alone like my son did that night.

I've worked with many States on similar legislation. I started a nonprofit speaking to teens about mental health and the dangers of Big Tech. I filed a lawsuit against Meta in January 2024, sold my businesses, and went to work for a tech company that provides tools to protect children. I've also become an advocate on the Hill, urging Members to see this as what it is, and that is, the greatest threat to the next generation.

In the 2 years of my advocacy, I've seen Big Tech lobby fight us every inch and Congress cave instead of listening to we, the people. I witnessed KOSA pass Senate 91-to-3, go to the House where the Speaker refused to let it be heard.

Senators Graham and Durbin have the DEFIANCE Act. Senators Blackburn and Coons, the NO FAKES Act. These are great bills. I've even taken notes and reintroduced them on a State level in South Carolina, like the ELVIS Act in Tennessee. Senators Cruz and Klobuchar led the TAKE IT DOWN Act, and has it already passed the Senate. I'd like nothing more than to be proven wrong about the inefficiency of Congress by having the House pass the TAKE IT Act soon.

Speaker Johnson, Chairman Guthrie, the ball is in your court with a bill to protect American lives. Please don't let us down, again.

I've witnessed over 40 teens take their lives since Gavin just due to sextortion, while we as lawmakers fight amongst ourselves. Will it take one of your own children or grandchildren to finally get fed up enough to move?

Sextortion is the only—is only one of the many harms due to our children due to Big Tech's lack of accountability. Big Tech is the Big Tobacco of this generation. We see groups such as NCMEC and NCOSE give statistics over and over. We see parent survivors knock on your doors daily, and Section 230 will go down as one of the greatest disasters, allowing Big Tech to run rampant without repercussions. We watch companies spend millions lobbying, fighting us in court, and continuously absolving themselves of responsibility.

In this very Chamber last January, I stood holding a photo of Gavin while Mark Zuckerberg offered a forced, pathetic apology. Where I'm from, we have a saying that says, "Don't talk about it. Be about it." And until these companies can be held responsible and the billions they make off of advertising to our children, Big Tech will simply never be about it.

I use this as an example. Meta pulled down 63,000 accounts in 1 day in one country, just from Lagos, Nigeria, and just off of Instagram. Now, ask yourself, did they pull those down to actually help our children? And if so, why haven't they done more since? Or did they pull it down for a PR stunt? I beg to say that that is nothing more than a PR stunt so they can get that pat on the back, as if they are doing something good—but have done nothing since.

I got way offline. But I want to focus on my main message to Big Tech. As lawmakers, I think we have to say, either get in line or get offline. And right now, we have too many politicians making decisions based on their next election and not enough leaders making decisions based on the next generation. Are we politicians? Or are we leaders? We can't just talk about it. We have to be about it. And if we can't protect our next generation, then what are we even fighting for? Tomorrow needs you, and our children need you now.

[The prepared statement of Representative Guffey appears as a submission for the record.]

Chairman GRASSLEY. Ms. Goldberg.

**STATEMENT OF CARRIE GOLDBERG, FOUNDER,
C.A. GOLDBERG LAW FIRM, NEW YORK, NEW YORK**

Ms. GOLDBERG. Chair Grassley, Ranking Member Durbin, and distinguished Members of the Senate Committee of the Judiciary, my name is Carrie Goldberg, and I'm a lawyer who represents families catastrophically injured by Big Tech. I want to tell you about a few of the cases I've been working on for the past decade.

I'm the originating attorney in a case against Snap where our client's children were matched with drug dealers and sold counterfeit fentanyl-laced pills that killed them. The case now has 90 families in it from all over the country, including families that you heard from last week. And I'm also joined by my client, Amy Neville, the mother of 14-year-old Alexander Neville.

In another case against Snap, criminals are exploiting a known security vulnerability to access CSAM and blackmail and extort kids with it. Yesterday, the ninth circuit dismissed one of my cases

representing a 15-year-old severely autistic boy who, at age 15, was funneled into Grindr's marketing campaign and was recommended to 4 different pedophiles who raped him over 4 consecutive days. In court, Grindr's lawyers said that they had no duty to restrict children's access to their hookup app.

In another case of mine, a 13-year-old, L.S., was lured to the site BandLab, another site with no age restrictions. She thought she was meeting a 17-year-old boy, but it turned out to be 40-year-old Noah Madrano from Portland, Oregon. He posted openly on this music-sharing platform songs about her called—one called "Pedophile in A Minor"—a song called "Pedophile in A Minor." On June 24, 2022, Madrano drove 15 hours to her home, abducted her on the way to school, stuffed her in the trunk of the car, and raped and abused her for 8 days. Despite there being a national manhunt, BandLab refused to provide law enforcement with key information that could have led to her fast rescue. They wanted to respect Madrano's privacy, they said.

Finally, I represent the family of 16-year-old Aidan Walden from Colorado, who, in July 2020, discovered a website that glorifies suicide, and learned on that website about a product that he could buy from Amazon and get Prime delivered to him and use it to end his life. Two months later, his grieving mother exchanged 57 messages with Amazon telling them about their product being amplified on a suicide message board. And yet Amazon, despite knowing there was no household use for this product besides suicide, continue to promote, sell, and deliver it for 26 more months. I now represent 27 other families who bought it after Amazon sold it to Aidan Walden and heard from his mother.

In all of my cases, tech has two main defenses: Section 230, and that they didn't know. Now, I was here a year ago with my clients, including Amy, when this Committee so powerfully told the CEOs of Meta, Twitter, Discord, Snap, and TikTok that you were done with discussions and you wanted solutions. The most important thing I can say is that families want legislation like KOSA, sunseting Section 230, the DEFIANCE Act, SHIELD. They want laws that increase accountability, that create protection boards at the FTC, the Cyber Tip Line, create procedures to contest a platform's failure to remove CSAM. They want injunctive relief. And families want civil remedies against platforms when they've increased the risk of harm.

Now, take for example my case representing A.M., one of the first cases to overcome Section 230 on trafficking and product liability. At age 11, A.M., lived in a normal town, living a normal life in Michigan when she went to a sleepover and discovered a website called Omegle. It matches strangers for private live-streaming. Omegle matched her with a man who made her his online sex slave for 3 years—extorting her, making her at the beck and call of he and his friends to perform for her, sometimes interrupting her at the dinner table or at school, even forcing her to go back on Omegle to recruit more kids. The abuse eventually ended when his home, which he shared with his wife's daycare, was raided and images of A.M. and other young girls were found.

In that case, Omegle did not intend my client's injuries. I could not claim that they knew who she or the offender was. Instead, I

pointed to the mountain of evidence that Omegle had, knowledge of how prevalent the harm was on its platform. I pointed to criminal cases, articles, exposés, academic journals.

And I just want to say two more things. As a result of how we pled the case, we advanced into discovery and acquired 60,000 documents exposing the extent of injured children. And that led to them agreeing to shutter Omegle forever on November 8, 2023.

Now, we are at a consensus today. We are all here to not repeat history. Section 230 was supposed to incentivize responsible content moderation. Instead, it did the opposite. And as we look into the future, on behalf of the victims I represent, we are here to support laws that pressure platforms to know about the harms and to fix them.

Thank you, and I look forward to questions.

[The prepared statement of Ms. Goldberg appears as a submission for the record.]

Chairman GRASSLEY. Thank you, Ms. Goldberg. Now, Professor Leary.

**STATEMENT OF MARY GRAW LEARY, PROFESSOR
OF LAW, CATHOLIC UNIVERSITY OF AMERICA
COLUMBUS SCHOOL OF LAW, WASHINGTON, DC**

Professor LEARY. Thank you, Chair Grassley, Ranking Member Durbin, and all the Members of this Committee. As has been mentioned, I'm really grateful for all the work this Committee has done on this issue. The experience our children are having in the digital space is one fraught with danger for them. And one might want to ask, why do you have to work so hard? Why do you have to keep passing these laws? Why are not the laws that Congress has had on the books regarding exploited crimes working?

And there's lots of answers to that to be sure. But the common thread through this morning so far is Section 230 of the Communications Decency Act, which has transformed—which has been transformed into what I label a de facto near absolute immunity regime. And what I mean by that is exactly what Ms. Goldberg just said. This was a law that was designed to incentivize platforms for protection. And instead, it has incentivized them to harm.

I want to make about five points that I think will help frame our discussion about Section 230. The first two are what I call framing principles. When one reviews the text, the history, the structure of Section 230 of the Communications Decency Act, it is clear that this is a law that is not stand-alone law protecting freedom of the internet as tech and its surrogates will try to argue. It is a law that is born out of a landscape of child protection. When you go back to the legislative history, there is no question the Senate with the Communications Decency Act, the House with the Internet Freedom and Families Act were wrestling with the same question. How, as you look to the Telecommunications Act, how could you, as Congress, have a safer internet and other media for youth? Not whether, but how? First point.

Second point, Section 230 of the Communications Decency Act must be regarded as an experiment. And I say that because when you look at the promises tech made back in 1996, and when you look at the supporters of the IFFE in the House, what you see is

they represented to you and to America that this would be a way in which we could protect our children. That was their claim. That was the promise.

Point number three, the experiment has failed. The experiment has failed for all the reasons that have been said already. And why has it failed? And I would say to you, in addition to the reference to what happens here in Capitol Hill with regard to tech, the transformation of section 230 of the Communications Decency Act into a law that incentivizes harm was not by accident.

It wasn't sort of something that just emerged from the internet. It was a systematic effort by tech and its surrogates to litigate that throughout this country. And they went across the country over 30 years arguing not for the narrow, limited protection for Good Samaritans that the Act states, but rather broad immunity. Interestingly, immunity is nowhere in Section 230 of the Communications Decency Act, as a side note.

That is—and that result has had human consequences, which we've heard today. And I think to highlight one that's been said, 99,000, 100,000 reports today will happen on the Cyber Tip Line. But it also has important effects in the courtroom that Ms. Goldberg alluded to, and I want to highlight a couple of them. One is, keep in mind this has become an immunity, not a defense, and that is essential for two important reasons. First, as an immunity, these cases are thrown out in a motion to dismiss, so there's no access to discovery.

So when we say that victim survivors, States' attorneys general are shut out of the courtroom, we don't mean it's very hard to win these cases. We mean they are shut out of the courtroom, that they do not have their day in court, notwithstanding the harm that they've experienced. And I label this reality, the dual danger of de facto near absolute immunity.

First, that shield, which has allowed platforms to engage in a list of criminal activities having nothing to do with publishing, that has allowed this industry to grow to a massive scale where one individual or one small company can cause massive harm, as we've heard. But the other part of that dual danger is, because it is an immunity, there is no access to discovery. There is no way to look under the hood of this incredibly dangerous industry. There's no guardrails. And that means that—as Senator Klobuchar pointed out—what that tells us, as I wrap up, is that there is no guardrails for the harm that these folks will experience.

So I offer some suggestions of reform in my papers. But I think the key thing here is to keep the Good Samaritan protections that Section 230 has, but to get rid of the (c)(1) protections that have so distorted this incentivization for harm.

And I would just encourage the Senate to listen to the words of Justice Thomas, where he has lamented about the reality of Section 230 and stated, "Make no mistake about it, there is danger in delay," and that danger we can do, with the math. If we accept that 99,000 reports of NCMEC will be made today, that means that 12,375 reports will come in during this hearing. And in the last 5 minutes I've spoken, there have been 344 reports. And if that's not reason to act enough, I don't know what is.

Thank you, Chair.

[The prepared statement of Professor Leary appears as a submission for the record.]

Chairman GRASSLEY. Thank you, Professor.
Now, Mr. Pizzuro.

**STATEMENT OF JOHN PIZZURO, CHIEF EXECUTIVE
OFFICER, RAVEN, IRVING, TEXAS**

Mr. PIZZURO. Chairman Grassley, Ranking Member Durbin, and distinguished Members of the Senate Judiciary Committee, thank you for the opportunity to testify today. As the CEO of Raven, an organization dedicated to transforming the Nation's response to child exploitation, I am here to urge decisive legislative action. Despite multiple testimonies before Congress, progress has been slow, hindered by special interest groups and financial incentives that favor the status quo. We must prioritize our children's safety and support those who protect them, above all else.

New threats continue to emerge while old ones remain unaddressed. Artificial intelligence now enables offenders to manipulate regular images of children into explicit content, create images of children who do not even exist, and groom children at mass. Offenders now increasingly exploit children for financial gain in addition to their depraved sexual gratification. Yet legislative inaction allows this crisis to persist. The tech industry has not meaningfully reduced online victimization. Their voluntary cooperation with law enforcement is minimal, allowing offenders to continue exploiting children with impunity.

In 2023, for example, there were 36 million cyber tips, yet Apple, holding a 57 percent market share in the U.S., only reported 275. According to investigators in the field, Discord notifies users of legal process and subpoenas, enabling offenders to erase evidence before law enforcement can act, allowing offenders to continue to target our children.

Electronic service providers permit offenders to rejoin platforms under new aliases with the same IP address while failing to block foreign IP addresses used for sextortion. This lack of enforcement emboldens criminals and leaves our children unprotected. Poor moderation, the lack of parental controls in relation to age identification, and inadequate safety measures further expose children to these dangers.

As mentioned a lot today, social media algorithms push harmful content, enabling predators to reach victims globally. AI-powered grooming will allow offenders to manipulate children at scale, mimicking their language and behaviors to establish trust. Troubling, even ChatGPT-like tools can provide information on grooming tactics when framed in seemingly innocent ways.

These dangers extend beyond child exploitation to drug access with platforms facilitating the sale of fentanyl and illicit substances. Law enforcement is overwhelmed and under-resourced. Undercover operations have been highly successful in apprehending offenders, but the increasing volume of cyber tips has made proactive investigations nearly impossible. In the U.S., there are 229,000 IP addresses currently right now trading peer-to-peer images of known child sexual abuse material, yet only 923 are

being actually worked. Studies indicate that over 50 percent of those individuals are hands-on offenders with 8 to 13 victims each.

The mental toll on those who investigate these crimes is severe. Prosecutors, child advocates, and law enforcement officers are exposed to daily horrific content leading to burnout and PTSD. We must provide them with adequate wellness resources to ensure they can continue their critical work.

As a retired New Jersey State Police commander, I have seen firsthand what can happen. Despite its critical role, the Internet Crimes Against Children Program, ICAC, has been chronically underfunded, despite being responsible for most of the child investigations in the U.S.

While authorized for \$60 million in 2008, only \$31.9 million has been appropriated. That's \$522,000 per task force per year to investigate child exploitation. That's why I urge everyone here to co-sponsor the PROTECT Our Children Reauthorization Act of 2025.

Children are our most valuable resource, and their victimization has lasting consequences on society. Raven stands ready to collaborate with Members of the Senate, House, Trump administration, and the CEOs of Big Tech to develop effective solutions. Quite frankly, the phrase "talk is cheap" is a 100 percent accurate. Action is only—the only remedy. How many of our children and those who protect them will be impacted as a result of our inaction and debate? Make no mistake, right now, offenders are winning, children are suffering. Those fighting to protect them are left to struggle without the support they need to rescue victims, hold offenders accountable, and bolster their own mental health in the process.

Legislative action is overdue. The solutions are within your power. Our children are counting on you, and I'm counting on you. Thank you so much.

[The prepared statement of Mr. Pizzuro appears as a submission for the record.]

Chairman GRASSLEY. Thank you, Mr. Pizzuro. Now, Mr. Balkam.

**STATEMENT OF STEPHEN BALKAM, FOUNDER
AND CHIEF EXECUTIVE OFFICER, FAMILY
ONLINE SAFETY INSTITUTE, WASHINGTON, DC**

Mr. BALKAM. Good morning, Chairman Grassley, Ranking Member Durbin, and distinguished Members of the Committee. Thank you very much for the opportunity to speak with you today. My name is Stephen Balkam, and I'm the founder and CEO of the Family Online Safety Institute. For nearly two decades, FOSI has worked with industry, government, academia, and the nonprofit sector to create a safer digital world for children and families. I'm also here as a father and a newly minted grandfather.

Chairman, this is my third time testifying before this Committee, having first appeared in July of 1995, a Committee hearing called "Cyber Porn and Children." While much has changed, our mission remains the same. We believe in a three-pronged approach to online safety: enlightened public policy, industry best practices, and good digital parenting. Our goal is to create protections for kids, as well as empower young people to navigate digital spaces safely and responsibly. We want to protect kids on the internet, not from it.

Parents of younger children should have the strongest protections possible, including easy-to-find and easy-to-use parental controls. But as kids grow, our role as parents shifts from being helicopter parents to copilots, guiding them as they build digital resilience. Research shows that teens value online safety tools like blocking, muting, reporting, and privacy settings. Teaching them to use these effectively fosters independence and self-regulations. We have found that empowerment is often the best form of protection. We must prepare young people to engage safely and thoughtfully with the digital world, equipping them with digital literacy and an understanding of their rights and responsibilities.

Now, recently there have been calls to ban young people from social media and other online spaces. Blanket bans deprive children from any positive experiences they may have, are difficult to enforce, and open up too many possible unintended consequences. After all, children have rights, including the right to safely access the web, to information, free expression, and to connect with others. Instead of blanket bans, we need thoughtful restrictions that include input from young people and that account for children's evolving maturity.

While technical solutions such as age assurance are improving, there is no universally approved system as yet. It is challenging to get the balance between safety, privacy, and effectiveness right. And as I said recently at our annual conference in front of 350 industry leaders, quote, "You can and must do better to create easy-to-find and easy-to-use controls for parents and online safety tools for teens and young people. You can and must do better to publicize and promote those controls and tools. And you can and must do better to collaborate with each other to harmonize your tools across the ecosystem so that parents and teens are not overwhelmed with the task of setting and managing controls across countless apps, games, websites, and social media platforms," unquote.

In the meantime, Congress has taken some important steps in this space, passing COPPA 27 years ago and the CAMRA Act three years ago, which funds essential research on children's development and well-being. But there's still much more work to be done. Federal action is critical because States are now beginning to fill the gaps with their own online safety laws. Unfortunately, even the most well-intentioned laws often face legal challenges and create a fragmented regulatory landscape. A strong Federal framework would provide clarity while allowing States to build upon this.

So, Congress has the opportunity to lead with balanced and thoughtful policies, including passing a comprehensive data privacy law, funding ongoing research to inform evidence-based policy-making, prioritizing specific targeted bills like the TAKE IT DOWN Act and the Kids Off Social Media Act, encouraging industry cooperation to simplify parental controls and online safety tools, rejecting blanket bans in favor of thoughtful restrictions that include young people's input, and, critically, supporting digital literacy programs to build resilience in young users.

So, to conclude, let us challenge ourselves to reimagine what online safety can look like, not just as a range of restrictions, but as a foundation for resilience, confidence, and opportunity.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Balkam appears as a submission for the record.]

Chairman GRASSLEY. Thank you all for your testimony. We'll have 5-minute round of questions. I'm going to start with Mr. Pizzuro.

AI has opened up new possibilities for bad actors to generate novel forms of CSAM. In fact, one recent report found that over 3,500 AI-generated CSAM images were posted in a single dark web forum over a 9-month period. Could you explain the challenge that AI-generated CSAM poses for law enforcement and tech companies?

Mr. PIZZURO. Well, there's a couple of things. One, right now, it's going to be hard to tell the difference, especially without forensic software, what is AI and what isn't. Second, I could just take my phone now, take a picture of a Senator, and then I can age regress them. For example, I can—you can be a 40-year-old male. I can now make you a 21-year-old female, and now I can make you a 10-year-old girl. And with that, and AI within these apps, I can actually then nudify those apps. So I think the challenge that comes with this and AI, especially from sextortion, I don't even need to groom someone right now. I can just get an image off the clear web in order to do that. So that's going to be the complexity, and the challenge is going to be is, how do we determine who is a real victim and who's not—in a lot of instances.

Chairman GRASSLEY. Thank you.

Professor Leary, 230—well, first of all, I heard your five points, so I'm not asking you to repeat any of them, but how would you advise reforming Section 230 in light of the current online ecosystem?

Professor LEARY. Thank you, Senator. Well, first, as I say, when we talk about Section 230 and the provisions that Tech points to, there's this, as this Committee well knows, (c)(1) and (c)(2)—(c)(2) is the Good Samaritan provision, and I would recommend that that stay in place. That incentivizes a platform to be able to remove harmful material from their platforms without being sued.

The (c)(1) part of the statute should be removed. As has been pointed by so many of you in your opening statements, it serves no purpose, if it ever did. Now, a myth has been created about it, that it somehow created the internet, and somehow the internet will break without it. And that's just simply not true. And if it ever was true, this is no longer a fledgling business that needs that kind of support. Instead, it needs to be treated like every other business.

Another important thing I would encourage the Senate to do with Section 230 is to listen to the National Association of Attorneys General who repeatedly has written and asked Congress to include in it the ability for them to enforce their State laws, which has also been ruled to be something that they cannot do when these courts—when Tech has argued for an expansive interpretation of Section 230. In my mind, that is another courthouse door that is closed. It's a States' rights issue. And the entire architecture of combating exploitation of our children is—involves prosecution, protection, and prevention, and within that involves multiple pressure points, including civil litigation, State prosecution, and Fed-

eral prosecution. And that, I think, would be an important amendment.

Chairman GRASSLEY. Mr. Pizzuro, obviously, it has taken a long time, and maybe it will take a longer time for Section 230 to be reformed, and also putting some more things in that can slow the process up. Beyond that reform and liability for Big Tech, what steps could companies take to protect children online today?

Mr. PIZZURO. Well, one of the things that they know is they know—for example, I had mentioned in my testimony, Discord, they notify users. They notify users when they get legal process. You know, those are certain internal policies. They know what IP addresses that there are because if I get banned, I just create a new username. So those are associated IP addresses. There's also IP addresses, you know, beyond the scopes of the U.S. where children are targeted here. So these are things that the companies actually know and can do something.

Chairman GRASSLEY. Professor Leary, the bills reported out of Committee last year that would impose liability on a platform for knowingly promoting CSAM and others for recklessly promoting CSAM, as we continue workshopping bills in this Committee, do you believe we should pursue a recklessness standard or a knowing standard and the pros and cons?

Professor LEARY. Thank you. I absolutely believe a recklessness standard is superior to a knowing standard. And again, you know, the—Senator Durbin referred to the red herrings. One red herring that's out there is recklessness is some very low standard that will somehow expose these businesses to an onslaught of litigation. A couple of comments on that. First, most businesses function having to act responsibly, and they face often a negligence standard.

Anybody who says that recklessness is an easy standard to make, I invite you, please, come to my criminal law class and meet my criminal law students who will be able to tell you the definition of recklessness, and they will tell you that it is challenging. And, specifically, it is a conscious disregard of not just a risk, a substantial and unjustifiable risk. That is the definition of recklessness in the criminal context, and it can be used in other contexts, as well.

That requires not just an objective measure, but a level of subjectivity. It's referred to sometimes as risk creation. So that kind of standard is hardly a day in the park for litigants. It is still quite challenging, and that's why it is a far better standard than knowingly, in my opinion.

Chairman GRASSLEY. Okay. Senator Durbin.

Senator DURBIN. Representative Guffey, thank you for coming back. I'm sorry for the circumstances which bring you, but it shows real courage, and I know your family and friends have joined you—

Representative GUFFEY. Thank you.

Senator DURBIN [continuing]. In coming here today. I recall the first time we met after a hearing a year or so ago before this Committee, so thank you very much.

Representative GUFFEY. Thank you.

Senator DURBIN. Mr. Chairman, was it a week or 2 weeks ago we had a hearing on fentanyl?

Chairman GRASSLEY. Yes.

Senator DURBIN. Yes.

Chairman GRASSLEY. Last week.

Senator DURBIN. And we had another parent of a victim who ordered what he thought was a Percocet, turned out to be laced with fentanyl, and took his life. So this is a life-or-death proposition that we're dealing with here, and you've lived it—and living it still. I think we ought to keep it in that context.

Professor Leary, I am struck by one of your statements that you've given to the Committee, that this notion that we are preparing 230 as an immunity as opposed to a defense precludes evidence being gathered and discovery taking place. And you say in your remarks to the Committee that that diminishes our knowledge of the actual goings-on at these tech companies and what they're doing and gathering. I recall what Representative Guffey said in his opening remarks, "This is bigger than Big Tobacco."

I know that issue. Over 30 years ago in the House, I introduced a little bill to ban smoking on airplanes. It passed because Congress is the biggest frequent flyer club in the world, and we were sick of it. And it triggered a conversation and a discovery process, and AGs from across the country gathered together and did something significant with this industry.

So I'd like you to expound a bit, if you will, as to how this standard precludes our knowledge of what's actually going on in Big Tech in their response to this challenge. I think that the gathering of that information for the tobacco companies, the demonstration of their lying to the public about the safety of their product, for example, really led to their downfall. I think the same could be true here.

Professor LEARY. Thank you, Senator. I think that you are 100 percent correct on that. When a defendant has a defense, as many—as I know the Committee knows, but to be responsive to the question, there's a period of discovery beforehand where—

Senator DURBIN. Like contributory negligence.

Professor LEARY. Exactly, exactly, or things of that nature. There's a period of discovery where the plaintiffs can—who've made a good faith claim can get information to build on their case, and the defendants can also provide information which may exculpate them.

The way that Section 230 has been interpreted, it is an immunity. And so prior to discovery is when these platforms are coming into court and saying, "Judge, we don't have to defend ourselves. We don't even have to litigate this case. You should dismiss it now," motions to dismiss prior to discovery. The only way that I would say the public has learned a lot of the information about Big Tech, for example, that I believe led to KOSA and some of the other duty of care, has been through what? Congressional investigations. I'm reminded of the Backpage, a congressional investigation, which was a 2-year investigation—or whistleblowers and hearings. That's how we are learning this information. And only by getting this information can we then make informed choices about what's the appropriate legislative text.

If I could just say quickly, Justice Thomas commented on this, and he has underscored this when he said, look, let's keep in mind, if we fix Section 230—that's not exactly what he said, but after

that he said, quote, “It would simply give plaintiffs a chance to raise their claims in the first place. Plaintiffs must still prove the merits of their case and some claims will undoubtedly fail. But States and the Federal Government will be able to update their liability laws to be more appropriate for an internet-driven society.”

Senator DURBIN. If I can make one final point in the closing seconds here, going back to my analogy, smoking on airplanes and ultimately dealing with the tobacco issue in a much larger context, the initial bill that I introduced and passed in the House banned smoking on airplanes on flights of 2 hours or less.

People said, what are you talking about? If it’s dangerous, it’s dangerous regardless of the duration of the flight. The reason was, I had a Minnesota Congressman who was a chain smoker who was holding up my bill——

[Laughter.]

Senator DURBIN [continuing]. And I went to him, he’s——

Senator KLOBUCHAR. It’s so timely that I arrived.

[Laughter.]

Senator DURBIN [continuing]. I went to him and I said, “Marty, how long can you go without a cigarette?” And he said, “Two hours.” So I put that in the bill, and he didn’t object to it, and it moved forward. There are things that we’re dealing with in some of these bills, which are compromises to try to move the issue forward, to make progress toward our goal. So don’t assume that any language is final. It is all in flux and subject to negotiation. But thank you for joining us.

Chairman GRASSLEY. Senator Lee.

Senator LEE. Thank you, Mr. Chairman. First, I’d like to thank all the witnesses for being here and for testifying on this important issue. These are not easy issues to talk about and not easy in particular because of the tragic circumstances that have regrettably brought you here.

Representative GUFFEY, I want to express my sympathy to you for the loss of your son, Gavin. No parent should ever have to go through that, and I want to commend you on your courage and the strength that you’ve shown as you continue to fight to protect all children.

Representative GUFFEY. Thank you.

Senator LEE. And, Ms. Goldberg, with what you’ve gone through, likewise, my heart goes out to you and to anyone else who has experienced the things that you’re describing.

For the past several years, I’ve strongly advocated for reforming Section 230 of the Communications Decency Act. And this is due to increasing concerns about how social media platforms are operating and how they’re utilizing Section 230. The platforms have enabled child sexual exploitation and promoted harmful challenges to children and facilitated drug trafficking—in many cases to minors.

Now, first, I introduced the PROTECT Act on this point, which mandates stricter safeguards on websites hosting pornographic content. Victims of online exploitation have faced an uphill battle for years, struggling to get online platforms to remove images that were nonconsensually obtained. The bill would require platforms to verify the age and also obtain verified consent forms from individuals uploading and appearing in content. And the bill would re-

quire tech companies to take stronger measures to prevent the exploitation occurring on their platforms and force immediate removal of child sexually explicit material and revenge porn upon receiving notice that the content in question was uploaded without the legally required consent.

Second, I introduced another bill as a complement to the PROTECT Act called the SCREEN Act. The SCREEN Act would require all commercial pornographic websites to adopt age-verification technology to ensure children can't access the site's pornographic content.

In the 20 years since the Supreme Court last examined this issue in earnest, technological advances have demonstrated that prior methods of restricting minors' access to pornography online were ineffective. Nearly 80 percent of teenagers between the ages of 12 and 17 have been exposed to pornography. This is especially alarming, given the unique physiological effects that pornography has on minors—effects that are much better understood and to a much more alarming degree today than they were 20 years ago.

Finally, I introduced a third bill called the App Store Accountability Act, which would prevent underage users from downloading apps with pornography, extreme violence, and other harmful content, while making it easier for parents to sue the gatekeepers of the content in question. Technology has advanced significantly over the last two decades. Modern age verification technology is now the least restrictive, least intrusive, and most effective means to which Congress has ready access to protect our children from exposure to online pornography.

Ms. Goldberg, if it's okay, I'd like to start with you. In your view, should app stores such as the Google Play Store and Apple's App Store be held legally accountable for allowing minors access to harmful content?

Ms. GOLDBERG. A hundred percent, app stores should have a duty. They are just a seller in this situation, and as we've said in our cases against Amazon, there's standards of seller negligence. So if you know that you are selling an unreasonably dangerous product, then there's liability.

Senator LEE. Liability. Liability that's in there would be if you sold a tangible physical object unsuitable for minors to someone with knowledge or reckless disregard for their age.

Professor Leary, do you believe requiring pornographic websites to adopt age verification technology for visitors and for all people featured on those websites in pornographic images, while imposing serious consequences for uploading and hosting nonconsensual pornographic content, do you think these are things that would help children?

Professor LEARY. I do think age verification—obviously with any piece of legislation, the words matter, but the idea of anything that will create friction between children and their exposure to pornography is an important thing, and age verification can be one of them.

I think the danger here is to suggest—not to suggest. The danger here is what I see is tech directing things away from them, often right as there's the solution—when we have to have a multi-tiered, multi-level approach. And that's why a combination of all of the

Acts you've talked about—the SHIELD Act, the DEFIANCE Act, the TAKE DOWN—TAKE IT DOWN Act, the NO FAKES Act—all together really provide much more protection than one or two approaches.

Senator LEE. Thank you.

Chairman GRASSLEY. Klobuchar.

Senator KLOBUCHAR. Thank you, Grassley.

[Laughter.]

Senator KLOBUCHAR. It is wonderful to be here and to hear your incredible testimony. I got through three of you, I think, and I first want to lead with you, Representative Guffey. Watching your family behind you and friends, how difficult this must be and how heartfelt your testimony was. I don't know how anyone can listen to you and not want to get something done here. So I want to thank you for that.

You've described how victims of these crimes often suffer from mental health trauma. Can you quickly elaborate on why even the threat of the nonconsensual distribution of explicit images can be tragic?

Representative GUFFEY. The threat is the most dangerous part of it. Not even the sharing of the images themselves are as bad of the threat because you are taking your deepest, darkest shame, or your most private moment, and the threat of sending it out to complete strangers is complete vulnerability. And I believe that in this country, we've lost grace, and we have too often kicked people for the mistakes that they make. And we tell our kids that everything you do online will stay with you forever. Well, imagine if you just took your darkest moment and just posted it online.

Senator KLOBUCHAR. Mm-hmm. Exactly. Federal—why should this be Federal?

Representative GUFFEY. Well, on a State level, I can tell you from passing—or submitting legislation, passing legislation, I have submitted things such as the PROTECT Act, the App Store Accountability Act. You know, we need help on a Federal level because Section 230 is causing States to go at this 20 different directions.

Senator KLOBUCHAR. Totally.

Representative GUFFEY. And until—if 230 isn't going to fix it, and the States are fed up on how ineffective Congress has been, we're going to continue to try to go at it any and every way we can. But it would be a whole lot nicer to have uniform code across the country instead of just protecting children in one State.

Senator KLOBUCHAR. Yes, like you might do with the airplane seat rules that I just brought up.

Representative GUFFEY. Yes.

Senator KLOBUCHAR. You don't have those State by State. That would be very difficult—

Representative GUFFEY. Yes.

Senator KLOBUCHAR [continuing]. To get any results.

Mr. Pizzuro, could you talk about why it's important that Congress pass these bills to give Federal law enforcement tools? As you know, Senator Cornyn and I have this SHIELD Act, which is really important, ahead of its time. And then the TAKE IT DOWN Act requires the platforms to take these down immediately, the non-

consensual images, but also make sure that there is criminal liability for those that are posting it. Could you talk about why that helps Federal law enforcement?

Mr. PIZZURO. Sure. The challenge becomes in investigating with—between State and Federal, there's a lot of gaps. So, as an investigator, there's areas where I can't successfully prosecute or have the actual law and order to facilitate things. So especially if you go to rural areas where there's not a State perspective, where there's not really good laws, not—you're going to need that Federal law and that aspect. So what SHIELD does, it fills that legislative gap—

Senator KLOBUCHAR. Mm-hmm.

Mr. PIZZURO [continuing]. In order for us to actually effectually do our jobs.

Senator KLOBUCHAR. Mm-hmm. Good point. And another question on the fentanyl and the drug track. The DEA recently found that one-third of fentanyl cases they investigated had direct ties to social media. Others, like the National Crime Prevention Council, estimate that 80 percent of teen and young adult fentanyl poisoning deaths can be tracked back to social media. It's not a statistic. It's actual lives lost. How do the design of an algorithmic recommendation by online platforms contribute to the facilitation of drug sales?

Mr. PIZZURO. Well, I could tell you this, even going back when I first started, not aging myself, but, you know, when there was cloned pagers and we were doing cartels—this is just the advent of technology. And with these tech companies and the AI algorithms, what they push, that's what they're going to see, so it doesn't matter. There is no—you know, one of the things—I asked Meta, I asked Snap, I asked a lot of these companies, "Can you explain your algorithms?" No one can and no one will because, again, it's about business. It's about pushing that content, and that's what children are seeing. So that's why they're at risk.

Senator KLOBUCHAR. Mm-hmm. Thank you. My last question of you, Ms. Goldberg, you have represented over 1,000 victims of revenge porn, just to give people a sense of those numbers. Of course, there's tens of thousands out there that never were represented. Can you discuss the challenges you face in getting justice for your clients and why passage of Federal laws like the SHIELD Act and the TAKE IT DOWN Act would make a difference?

Ms. GOLDBERG. Sure. When I started representing victims of revenge porn 10 years ago, there were three States that had laws. And everyone wanted to blame the victims and said, "You shouldn't have taken that picture in the first place." And it wasn't until we were testifying about it and, like, actually making people realize that the liability needs to be, like, in the hands of the offenders. There's a responsibility in being the recipient of it.

But the bigger problem, though, was that the platforms were the ones that were distributing the content at scale. So, you know, back in the old days, revenge porn could be, you know, photocopied and put on a car windshield. But now with Snapchat and Google and Meta, one picture can be seen by millions and millions of people, and we need the uniformity like Mr. Pizzuro was saying.

Senator KLOBUCHAR. Mm-hmm. Thank you. And I know my colleagues asked about Section 230, which I feel very strongly about, so I'll let that go. Thank you.

Chairman GRASSLEY. Senator Klobuchar, thank you. Senator——
Senator KLOBUCHAR. Thank you, Chairman Grassley.

Chairman GRASSLEY. Senator Hawley.

Senator HAWLEY. Thank you, Mr. Chairman. Thank you for calling this hearing. Thanks to the witnesses for being here.

Mr. Pizzuro, let me just start with you. You've been working in the anti-exploitation space for a long time, both inside and outside government. Have I got that right?

Mr. PIZZURO. That's correct.

Senator HAWLEY. And so you know the trends about what we're facing online, what kids are facing online, probably as well or better than anybody. Is that fair to say?

Mr. PIZZURO. I would say pretty so.

Senator HAWLEY. Would you say that that CSAM—Child Sexual Exploitation—or Abuse Material, would you say that there's getting to be more of it or getting to be less of it?

Mr. PIZZURO. Oh, a hundred percent more, like hundreds and thousands more. I mean, I can't even percentage it.

Senator HAWLEY. Yes, enormous amounts. Right?

Mr. PIZZURO. Yes.

Senator HAWLEY. Here's a measure of it——

[Poster is displayed.]

Senator HAWLEY [continuing]. In 2023, there were 104 million images and videos of suspected child abuse material uploaded onto the internet compared to 450,000 in 2004. So 450,000 in 2004 to 104 million in the last full year for which we have data.

Here's another statistic. According to the National Center for Missing & Exploited Children, the number of reports of child exploitation material went from 1 million in 2014 to 36.2 million in 2023.

Mr. PIZZURO. That's right.

Senator HAWLEY. So, in other words, it's just an enormous explosion. It's absolutely everywhere.

So let me ask you about some of the remedies for this. If you are a parent—and I'm the parent of three young children, three little kids. If you're a parent of a victim of child sexual abuse material and your child's image has been used, they've been exploited, it's been used online, and you've got companies who have hosted that content recklessly or intentionally or negligently, or—they've done it. If you're a parent, can I sue them and get them to take it down?

Mr. PIZZURO. Right now, no. You can sue them, but I don't know how successful you're going to be.

Senator HAWLEY. So if I went into court, if my kid is abused, their content is up online, we know the abuser, but we've got these companies that are hosting the content and making money on it by distributing it, and I go to the company, let's say I go to the company and I say, "This sexual abuse material—this is my kid. This is online. I'm reporting it to you. I want you to take it down." Let's say they don't take it down, you're telling me I can't go into court and sue them?

Mr. PIZZURO. Other—you're going to probably end up losing. I mean—and I think that's part of the problem.

Senator HAWLEY. It's a huge problem. Is it not?

Mr. PIZZURO. Yes.

Senator HAWLEY. You're exactly correct.

Mr. PIZZURO. Yes.

Senator HAWLEY. You're exactly correct. The state of the law is I cannot go into court and hold these companies accountable. In fact, we had testimony just a few weeks ago of somebody sitting right where you're sitting, a parent whose child was sold drugs, in this case over one of these platforms—over Snapchat. This parent went in, reported it to Snapchat. Snapchat said, "Oh, well, we'll do our best." They did nothing. The parent said, "I'm going to sue you," and the Snapchat executives laughed in her face and they said, "Oh, no, you're not. You're not going to sue us because Federal law prohibits you from suing us."

Let me just ask you this. In 2019, Facebook was fined by the FTC \$5 billion—\$5 billion—with a B, and their stock price went up. Now, what does that tell you about what these companies fear? Do you think they fear these Government regulatory agencies that almost never bring suits and almost never bring enforcement?

Mr. PIZZURO. Oh, absolutely not.

Senator HAWLEY. Do you think that they fear lawsuits from parents who might get into court and get a \$1 billion or a \$10 billion judgment?

Mr. PIZZURO. For them, it's the cost of doing business. Right?

Senator HAWLEY. Yes, exactly. And they're willing to pay it. Facebook paid that \$5 billion. Their stock price went up. They went right on doing what they were doing. But I tell you what they do fear, what they're absolutely terrified is, they're absolutely terrified of a parent coming into court and getting in front of a jury and holding them accountable. And that is why it is high time—it is past time that this Congress gave parents the ability to do that.

And I will just say, again, for the approximately three millionth time in this Committee, until Congress gives parents the ability to sue, nothing will change. These companies don't care about fines. They don't care about the regulations. In fact, the companies regularly come and sit here and offer to write the regulations. They say, "Oh, we're great public citizens. We'd love to help you write the regulations, Congress, and we promise to comply. We'll write them, and then we'll comply." They won't comply. They buy off the regulators. What they fear are juries.

And this is why what Senator Durbin has done with his bill that we worked on together to give parents the right to get into court and have their day in court is absolutely vital. And I'm proud to be working with him on this. It passed unanimously out of this Committee last year when he was the Chairman, and I look forward to reintroducing it. We make it even stronger, even better this year. But I just say, again, there is nothing more important that this Congress can do to stop this than to give parents the right and victims the right to get into court and to hold these companies accountable.

Thank you, Mr. Chairman.

Senator LEE [presiding]. Thank you. Senator Hirono.

Senator HIRONO. Thank you, Mr. Chairman. Thank you all for testifying. And, Representative Guffey, our hearts go out to you.

We have been here many times already. Yes, I agree that we have to do something about Section 230, but one of the things that Professor Leary mentioned—and before I get to that, by the way, enforcement is really important, and I just want to note that last week when I was questioning Mr. Blanche, who is President Trump's nominee for Deputy Attorney General, I noted that protecting children online is an issue that unifies the Members of this Committee, as you can see.

That is why I was disappointed—in his non-answer to one of my questions I explained that if we want to protect children, the last thing we should do is fire prosecutors who fight child exploitation and impose a hiring freeze that stops them from filling these vacancies. But that's exactly what's happening. So I think we should note the environment in which we are having this hearing. Moreover, there was a funding freeze briefly that cutoff funding to Internet Crimes Against Children Task Forces that fight child exploitation in every State.

So child exploitation is a multifaceted issue, and I want to get back to Professor Leary, who said that the States ought to have the right to go after child exploitation in court and that they are not able to do so because of Section 230. Does that cover both criminal as well as civil prosecutions by States?

Professor LEARY. It has been interpreted that way. The States—and the way it's been interpreted is there's language in Section 230 of the Communications Decency Act which talks about that no State—not supporting a State law that is in contravention with Section 230 of the Communications Decency Act.

So courts have interpreted that as, oh, that means you can't enforce your State criminal laws, which happened in the *Dart* case—which was an attempt in the *Dart* cases, and I assume it would happen in civil cases under the (c)(1) provisions of the statute.

Senator HIRONO. Well, so you would support legislation at the Federal level that would allow the States to enforce their own child protection laws?

Professor LEARY. One hundred percent. And I believe that my written testimony has a quote from the letters from the national attorneys general laying out, again, for the third time—and, again, speaking of unanimity, I believe there's—I don't know exactly how you can have over 50 attorneys general. I believe it's the territories as well—all in agreement on this point.

Senator HIRONO. And, Representative Guffey and Ms. Goldberg, you would agree that we need to do something that would enable the States to support their own laws?

Representative GUFFEY. I would certainly agree with that. I think that's one of the tools in the toolbelt. But yes, States need to be able to have the tools.

Senator HIRONO. For Ms. Goldberg, you noted very briefly the ninth circuit and their decision in a case that you were involved with. Could you provide some background on the case and how Section 230 was involved and what you think that this case demonstrates the state of the law around Section 230?

Ms. GOLDBERG. Yes. So that case is called *Doe v. Grindr*, and it accuses the dating app Grindr of advertising to children using Instagram and TikTok with child models in school settings and luring them onto the dating app. And, as I said in my complaint, there were—there's statistics that 50 percent of gay kids have—who are sexually active have their first sexual experience with an adult that they meet on Grindr.

Now, Grindr has no age verifications and just absolutely turns a blind eye to the fact—

Senator HIRONO. Mm-hmm.

Ms. GOLDBERG [continuing]. That there are so many kids that use their product and inevitably are recommended to adults.

Now, I claimed that this was a defective product, and Grindr, because they knew about the problem, as I stated in my lawsuit, and were not—and were refusing to institute any sort of age verifications, they were also condoning trafficking. And the case got thrown out by the district court, and that was affirmed yesterday by the ninth circuit. So I never got—

Senator HIRONO. So—

Ms. GOLDBERG [continuing]. To go to discovery.

Senator HIRONO [continuing]. It was thrown out because of Section 230 immunity?

Ms. GOLDBERG. Of Section 230 and because of the incredibly high knowledge standard of actual knowledge that was—that they were imposing, which they didn't have to impose, but they imposed in the trafficking claim.

Senator HIRONO. I support the general proposition—thank you, Mr. Chairman—that anyone who gets injured by someone else's actions ought to be able to pursue legal remedies. Therefore, you know, I agree that we need to remove Section 230 immunity somehow and still pay attention to various other unintended consequences that may flow from that kind of a change, but it's not where we ought to be because this is a growing problem.

Thank you, Mr. Chairman.

Senator KENNEDY [presiding]. Thank you, Senator. I believe I'm next.

Representative, I'm sorry. But your boy's proud of you. You're doing good work.

Representative GUFFEY. Thank you.

Senator KENNEDY. Now, my late father used to tell me that you'll never know love until you know the love of a child. And I didn't believe him, but I do now. I don't know what I'd do if something happened to my boy. I'm just so sorry.

Representative GUFFEY. Thank you so much.

Senator KENNEDY. Mr. Pizzuro?

Mr. PIZZURO. Sir?

Senator KENNEDY. Social media is now a big part of childhood. Isn't it?

Mr. PIZZURO. Yes.

Senator KENNEDY. Can we agree that big parts of social media have just become cesspools of snark?

Mr. PIZZURO. I can probably attest to that, yes.

Senator KENNEDY. Can we agree that social media has lowered the cost of being an a-hole?

[Laughter.]

Mr. PIZZURO. Yes.

Senator KENNEDY. Can we agree that big parts of social media have become cesspools of sexual exploitation?

Mr. PIZZURO. For sure.

Senator KENNEDY. And I assume you'd agree with me if I said that social media has lowered the cost of being a pedophile. Hasn't it?

Mr. PIZZURO. Absolutely. It made it easy access.

Senator KENNEDY. Yes. You're familiar with the National Center for Missing & Exploited Children's Cyber Tip Line?

Mr. PIZZURO. Yes.

Senator KENNEDY. Are the social media companies required to report instances of child sexual exploitation to the National Center?

Mr. PIZZURO. Of what they see.

Senator KENNEDY. Okay. So the law says the social media companies have got to report these instances of sexual exploitation to the National Center. First, they have to look. Don't they?

Mr. PIZZURO. Yes.

Senator KENNEDY. Do they make any money when they look?

Mr. PIZZURO. No. If you just look at the Apple statistics I gave before, out of, what, 36 million, there's 275 came from Apple, so—

Senator KENNEDY. But they're not paid to look?

Mr. PIZZURO. No.

Senator KENNEDY. Okay. In fact, they want people coming to their social media platform?

Mr. PIZZURO. More users, more money.

Senator KENNEDY. Yes. They want eyeballs so they can sell them advertising. So for them to look is inconsistent with their economic interest. Isn't it?

Mr. PIZZURO. Correct.

Senator KENNEDY. All right. Now, once they look and they find it, then they have to report it to the National Center. Is that right?

Mr. PIZZURO. That's correct.

Senator KENNEDY. Are they paid to report it to the National Center?

Mr. PIZZURO. Absolutely not.

Senator KENNEDY. Okay. How many instances—I know this is a difficult question. How many instances do you think are of sexual exploitation of children are occurring and not being either looked for and/or reported by the social media companies?

Mr. PIZZURO. Well, I don't have NCMEC statistics but I could tell you that most of—there's a lot of ESPs that don't actually even report. So some overreport, some don't report at all. So that's part of the challenge.

And then, secondary, it's voluntary, right, so whatever—

Senator KENNEDY. Right.

Mr. PIZZURO [continuing]. They give them, there's no uniformity in data as well.

Senator KENNEDY. Yes. What happens if they don't look and they—and/or they don't report? Are they punished?

Mr. PIZZURO. No.

Senator KENNEDY. Okay. You're familiar with the Safer program?

Mr. PIZZURO. A little bit.

Senator KENNEDY. Okay. It's a tool. They use AI to scan conversations and look for patterns that might be sexual exploitation of children. It's not the only algorithm out there. Do social media programs all use that?

Mr. PIZZURO. I don't know how many do, but—I don't know if they're using technology, but they should.

Senator KENNEDY. Are they required to use it?

Mr. PIZZURO. Nope.

Senator KENNEDY. We've got to do something.

This is my last question. Do you find it ironic that all of these people in Big Tech who dreamed about and talked about creating a utopia have managed to generate more hate and more harm than anyone could ever have possibly imagined, all to make money?

Mr. PIZZURO. And lots of money they made.

Senator KENNEDY. Do you find that ironic?

Mr. PIZZURO. Very.

Senator KENNEDY. Thank you all for being here.

Senator Blumenthal—he's not only next, he's the only one left. But it's nice to see him.

Senator BLUMENTHAL. Am I recognized, Mr. Chairman—Mr. Ranking Member or are you presiding?

Senator KENNEDY. I'm the Chairman.

[Laughter.]

Senator BLUMENTHAL. You're presiding?

Senator KENNEDY. I'm the Chairman, Blumenthal.

Senator BLUMENTHAL. That may be the reason I'm the only one left.

[Laughter.]

Senator KENNEDY. Could be. I'm looking forward to your questioning. And I'm going to turn the gavel over to Senator Blackburn.

Senator BLUMENTHAL. Thank you, Chairman Blackburn.

Representative Guffey, thank you for being here today, and I think our hearts go out to you. I know I'm not the first to have said it, but your courage and strength makes an enormous difference. I know how strongly you supported the Kids Online Safety Act, and I am deeply grateful to you for your support and your activism in going to Louisiana, for example, seeking to talk to Representative Scalise and Representative—Speaker Johnson on behalf of that bill.

You did an article that I would like to have entered into the record if there's no objection. And there seems to be none.

When you went to see Representatives Scalise and Johnson, were you given an opportunity to talk to them?

Representative GUFFEY. No, sir—myself or the other parents. We did meet with Representative Scalise's staff, which, of course, was in district at that time, but even coming up here to the Hill, unable to meet with either one of the Representatives.

Senator BLUMENTHAL. Would you like to meet with them?

Representative GUFFEY. I would love to.

Senator BLUMENTHAL. Well, we'll try to arrange it for you.

Representative GUFFEY. Thank you, sir.

Senator BLUMENTHAL. I'm hoping they'll hear from you. I'm hoping they'll support the bill this time. Do you agree?

Representative GUFFEY. I 1,000 percent agree.

Senator BLUMENTHAL. Why don't you tell us, as a parent—but also as a advocate and the author of that article, why you think some of the arguments made against KOSA based on a supposed free speech thesis are incorrect?

Representative GUFFEY. I believe it is all “follow the money.” If you look at Big Tech and their lobby and you look at the narratives that get put out there and you look at the Representatives that fight against it and you follow the money and where it ends up, I believe that that fear—and, as an elected official, you know, I see it myself. You're often worried about what this will look like.

And that's one of the reasons, whenever I was presenting, I used the phrase that we have too many politicians worried about their next election instead of leaders worried about the next generation. And I believe that it's a false narrative that has been put out there. The argument has been had over and over, and people will agree with you, and then they will turn right around and share a false narrative.

Senator BLUMENTHAL. I think the United States Senate has recognized that it's a false narrative through a strong bipartisan vote here, 91-to-3 in the last session. I'm hoping that we'll have that same kind of support again. And I thank my Republican colleagues, particularly Senator Blackburn, who has been such a steadfast partner in this effort.

I'd like to turn to Professor Leary. I think I misattributed the article to Representative Guffey, but maybe you can expand on his response on that free speech false narrative.

Professor LEARY. Sure. Thank you, Senator. So first thing about free speech—well, first, as you know, I believe the article you're referring to, the op-ed, myself and other scholars wrote this piece, and it really dispelled these arguments about KOSA and really that we see again. In fact, if you look back in history, it's interesting to look at what some of tech has said over the years. I can go back to 2014, they are making this argument. We can go back actually before that, to 1996. They told us the Communications Decency Act was going to ruin free speech. Then they said it about the SAVE Act, then they said it about SESTA, FOSTA and, lo and behold, we still have plenty of free speech.

The thing to keep in mind with free speech is—the First Amendment is—that is an Amendment designed to help inform us on how to handle these sticky issues. It is not a reason to not engage in legislation, and that—it's being used in that manner. There's a distinction between speech and conduct. And specifically with KOSA, KOSA addressed conduct, not content. And so the speech argument was particularly misplaced with regard to that piece of legislation.

Senator BLUMENTHAL. Thank you. In fact, KOSA affects the conduct involved in product design. There's no more limitation on free speech than there would be if and when—because it does—the Federal Government regulates the safety of the design of an automobile or a toaster or a washing machine. If they explode, there is liability for it. It's not free speech to design a defective and

harmful product. It's conduct. And there is no censorship, no blocking of content in KOSA.

Thank you all for your testimony today. Thank you, Madam Chair.

Senator BLACKBURN [presiding]. I thank you. And, Professor Leary, I'm going to stay right with you for my question. I appreciated so much that op-ed that you had put together and the difference that you're making there that it was not a free speech infringement. This is, as Senator Blumenthal said, product design, as you said, conduct. But we know the reason that Meta and Google and the groups lobbied—just millions of dollars spent lobbying against this—is because they have assigned a dollar value to each and every kid. And I think the dollar value is \$270. And so our kids are the product, and it is so unseemly. To me, it is absolutely disgusting that they devalue the lives of young people in this manner.

Mr. Pizzuro, I want to come to you. Senator Klobuchar and I have the National Human Trafficking Database Act which would establish a database at DOJ's Office for Victims of Crimes and incentivizes States to collect and to enter and share their data. What we're trying to do is get a full picture of what is happening in each of the 50 States when it comes to human trafficking. And we have really had a tough time doing this and finding those people that are behind these human trafficking rings. I know your organization, Raven—

Mr. PIZZURO. Yes.

Senator BLACKBURN [continuing]. Has been supportive of the bill.

Mr. PIZZURO. Yes.

Senator BLACKBURN. I'd like for you to talk for just a minute about why having a national database is so vitally important to breaking this modern-day slavery apart.

Mr. PIZZURO. Well, the more data we have, the more we're able to understand and see and react to. And I think that's part of the challenge is, that, as States, we're so fragmentized, so we're getting data from just certain areas. So the more data we're able to actually collect, the more likely we are able to put a comprehensive plan and understand how to go after, you know, certain trafficking.

Senator BLACKBURN. And I want you to touch for just a moment on the use of AI-generated CSAM because what we hear from law enforcement is they're having to sift through so many images to figure out what is AI-generated and what is actual.

Mr. PIZZURO. That's a challenge. So right now, you can't—a detective investigating something—I can't tell the difference between what a real image is and what is not a real image. So technology exists now I can make those images whoever I want. I can make a child from an adult. And the challenge really becomes is now I could take your images off the clear net, off of social media, off of open profiles, and then turn that person into a child or, better yet, have sexually explicit images. The challenge is going to be we can't see it unless we have the software capabilities in order to actually do that—which, again, we don't have.

Senator BLACKBURN. I appreciate that. And Senators Coons, Klobuchar, Tillis, and I introduced the NO FAKES Act to deal with AI-generated voice and visual likeness of individuals. And we think

that this will play an important role in a remedy for AI-generated CSAM.

Representative GUFFEY, I'd love to get your thoughts on that.

Representative GUFFEY. On the NO FAKES Act, I personally love it. I've actually resubmitted the use of a bill very similar within the State. But I love the idea of using the name, image, and likeness. I think that is a very easy thing to hit. And as we talk about using AI-generated pornography, one of the problems that we have is stating that this is not a real person, therefore, is it really a crime? Bills such as Name, Image, and Likeness protects our citizens as opposed to focusing solely on what the image is. It protects the citizens.

Senator BLACKBURN. Let me ask you this—and congratulations on getting Gavin's Law passed.

Representative GUFFEY. Thank you.

Senator BLACKBURN. Is there a way you can amend provisions of NO FAKES onto Gavin's Law and begin to expand the protections there at the State level?

Representative GUFFEY. In South Carolina, unfortunately, no.

Senator BLACKBURN. So it's going to be two separate, so you'll have to have—

Representative GUFFEY. Yes.

Senator BLACKBURN [continuing]. A group of bills—

Representative GUFFEY. Yes, ma'am.

Senator BLACKBURN [continuing]. That will do this. Okay. And I am over time. I am going to recognize Senator Schiff and turn the gavel to Ms. Moody.

Senator SCHIFF. Thank you, Madam Chair. Thank you all for being here. And, Mr. Guffey, I appreciate your advocacy and want to express my condolence for the loss of your son. I can't imagine the trauma that you and your family have been through. But I appreciate your taking that trauma and using it to protect other families.

I have not had a chance as a new Member of the Senate to really study the multiple approaches of the various bills, although some I've supported in the House. But I wanted to ask you, Professor, we established Section 230 for the reasons I think you implied, which is, it was a nascent industry. They urged us to do so, so that we would not stifle innovation. They also made the argument that, without 230, they would not moderate content because they would be sued if they did, and this would encourage them to moderate content. Well, there may have been a time where they moderated content, but those days seem to be over.

It certainly wasn't enacted because it was believed necessary for the First Amendment. The First Amendment stands on its own two feet. In the absence of 230, companies could still plead a First Amendment defense to any case. What is your preferred approach? That is, it a repeal of 230? Is it changing it from an immunity to some form of defense? Is it to cabin 230 in some way by narrowing the scope? What are the merits of the various approaches?

Professor LEARY. Thank you, Senator. I would say that it's important to—a couple of things. I would say that there was discussion in the deep background about this free internet nascent industry. And when we look at the policies and the findings at the begin-

ning of Section 230 of the Communications Decency Act, there is language as to that. But I would repeat, the overwhelming background and discussion was about the child protection piece. And therefore, I think that the concern—I think that better than repealing the entire thing is to keep the (c)(2) language, which gives a cover, gives a protection to a platform if they—and specifically, if they remove anything they consider to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, that will protect them. That’s all they need. They do not need (c)(1), which is what has been turned into this de facto near absolute immunity.

I think also adding the State’s ability to proceed is an important thing. I think outside of 230 is holding them liable when they host this material. That has been discussed at length as well. So I think that those and some of the other things that I’ve listed—but I don’t want to use up too much of your time—all work together to respond to the complex crime.

Senator SCHIFF. And, Counsel, in your representation of clients in this area, what do you believe would be most helpful in terms of making sure that you can get the discovery you need and that we have established the right protections and the right burdens in terms of the platforms and the pipelines?

Ms. GOLDBERG. Thank you. I agree. We are long overdue to just abolish Section 230. But what’s important is that clients need to get into discovery so that they can actually know what—you know, the extent of the problem. And the only way we can do that is if the standard is reasonable for parents to plead. If we have to show that the company knew about that picture or that exact victim, that exact perpetrator, there’s no way a client’s going to be able to overcome a motion to dismiss and get into discovery. So we need to actually have standards like negligence, which the law already affords in almost all causes of action.

Senator SCHIFF. So let me ask this question. I don’t think there’s any doubt that if a company has devoted their technological capability to trying to solve this problem, that they could make enormous gains. They wouldn’t be able to eliminate the problem altogether, but nonetheless, they could prove very effective. What would you propose the new standard be then? That is, if it’s not going to be possible to completely do away with this, the standard can’t be perfection, how would you define the standard of care that you would expect the industry to follow, given that it hasn’t had to follow any standard with the protections of 230?

Senator MOODY [presiding]. And if you could just quickly answer that.

Ms. GOLDBERG. Oh, sure. Well, these are products, so strict liability should apply here. If these companies have created a defective product, then all users should be able to sue them without having to even prove a duty if the product injured them.

Senator SCHIFF. Thank you.

Senator MOODY. Thank you, Senator. Appreciate you being here today. I have been so impressed with this Committee. I am a Senator all of 4 weeks, so get ready. I bring to it with an array of passions I have acquired, not just as an attorney general but as a mother of a teenager right now. And I’m so impressed with the top-

ics that we have focused on, and specifically this one. It was shocking to me that the Senate was able to move forward pretty unanimously on some protections for children, and they ran right into the House that did not go along with some of those things. And I'm hoping that we can change that.

As attorney general, obviously, I fought in court against many of the platforms. I investigated platforms for harms to children. I am the mother dealing with this now. In fact, I tell people all the time, it is really hard to be one of the first generations of parents trying to parent children, and we don't understand what we're doing because we don't understand the technology to the degree they do. In fact, when I'm going through some of the controls, I often have to ask my kid what that means, which seems to defeat the purpose. But here we are.

And while I can break down what we're addressing today by privacy concerns of children, certainly, harm to children, whether that is mental effects, addiction, or materials that they never would have been exposed to in the past but they now have ready access to, one of the things I want to talk about quickly is the access to our children by predators and bad actors. I think this is this third lane that we read about repeatedly in the paper every single day. In my State, from doctors to predators to you name it, they're getting access to our children. And parents in the past could lock our children's bedroom doors and know they were safe at night, but that is not the reality anymore. In fact, in my own child's school, there were five teenage boys. A woman was arrested for posing as one and luring them and molesting them online I think using Snapchat and TikTok.

And of course when you engage with the platforms, they will often deny that this is happening. But it is happening, and the best people that can represent that are the parents where it's happening to their children in their homes while they thought they were safe.

And so I really commend you, as a fellow parent, Mr. Guffey, for taking your pain and channeling that into just frustration and anger because that is what is going to get the attention of lawmakers. I mean, we've tried to get the attention of the platforms. We've talked a lot about what needs to be done to force some restrictions and them acting on their own, but we need to talk about what needs to be done through laws. And what I'm specifically concerned about—and I would open this up to whoever wants to answer this question. What is the thing that we can do as lawmakers right now to stop predators from getting access to our children?

Mr. PIZZURO. I could—okay.

Senator MOODY. Let me start down there, and then we'll come to you.

Representative GUFFEY. I want to use this as an example because the comment was made that we essentially have different laws for the outside world than we do for the inside world. If I had a storage facility and I stored only guns in there, and you as attorney general, and someone was breaking the law and I said, okay, the majority are law-abiding citizens, but we also have terrorists, and we're going to store guns for criminals. And if I told you that

you had to have the digital ID to get into that locker, you'd think that's ludicrous. But that's exactly the way that we treat CSAM.

I mean, to me, I believe that if you're housing CSAM, you should be held responsible. But nothing is going to change until we open up civil liability. These are the world's richest companies since the inception of man, and yet they are immune.

Ms. GOLDBERG. And I'd say that if you have designed a product where you are exposing children to predators and you can't stop that from happening, then it's a defective product. And all a parent or a victim should have to do to be able to sue you is just to show that you know about the problem and the extent of it.

Senator MOODY. And in your experience—and I understand that this has happened—when parents have demanded and shown that this harmful material is online and demanded that they take it down, they've now told them about it, they know about it, and there have been refusals to take it down.

Ms. GOLDBERG. Absolutely. And those cases get thrown out of court because the online platform says, well, I didn't know about that specific incident. You know, of course they're not going to know about that specific incident. Or they're going to say, I didn't intend to harm that exact child.

Senator MOODY. And, Mr. Pizzuro, I know you have law enforcement experience, and I'm grateful for that. Thank you. My husband is career law enforcement. Understanding that predators can now get to our children through online platforms and online, what is the number one thing you would recommend to prevent that, that we can do as Congress?

Mr. PIZZURO. Device-based age verification. You mentioned parental controls. If there was a framework for a parent just to shut the spigot off and make it easy, rather than go through 25 different apps. The companies have this. We can stop it at the device level. That's where we prevent children from getting onto some of these images and offenders getting access to those children.

Senator MOODY. Thank you. And since I am the Acting Chair, I don't want to exceed the boundaries of time, so I will turn it over to Senator Whitehouse.

Senator WHITEHOUSE [presiding]. Thank you. And I understand that I've been given permission to close out the hearing at the end of my questioning, so I know you have another place to be, so don't hesitate to go where you need to be.

First of all, Ms. Goldberg, you said that repeal of 230 was long overdue. I'm hoping that that day is coming fairly soon and that a bipartisan bill to do just that will be filed by a group of Members from this Committee before very long.

As you also pointed out, there are standards by which to evaluate the conduct—or misconduct of these big platforms that the law already affords, and everybody else has to abide by those same standards—if you're a radio station, if you're a newspaper, if you're a manufacturer, if you're an individual. Some of them go back to the English common law that came over with the first settlers. And the idea that what Representative Guffey described, I think quite well, as institutions that are the richest since the inception of man shouldn't be bound by the law.

I adore Ron Wyden. I think he's a wonderful Senator. He put Section 230 in when these platforms were in people's garages. And they've gone from that to being the richest companies since the inception of man—I'm not going to forget that phrase of yours, Representative Guffey. I like it—with no change in Congress' response to the original rationale for having that Section 230 protection and also repeated grotesque failure by these entities to police themselves. It's not as if we're dealing with a array of platforms that have a demonstrated record of meeting the public interest in the safety of their product. Not at all.

As a—lawyer to lawyer, Ms. Goldberg, talk a little bit about when the Section 230 defense first kicks in and what that means in terms of you and your clients actually being able to get discovery, to take a deposition, to find out the truth of what actually transpired.

Ms. GOLDBERG. What happens is that I file a lawsuit with all my facts, with everything that I can know, even though there's so much asymmetry of knowledge. Like I don't know the extent to which the platform knows about the exact problem or the overall problem. I can just base it on what's happened to my client, if they're alive. Otherwise, I have to go through their parents. So immediately, within like 30 days—

Senator WHITEHOUSE. So you file your complaint—

Ms. GOLDBERG [continuing]. They—

Senator WHITEHOUSE [continuing]. You state a claim—

Ms. GOLDBERG [continuing]. They file a motion—

Senator WHITEHOUSE [continuing]. And then they file—

Ms. GOLDBERG [continuing]. To dismiss—

Senator WHITEHOUSE [continuing]. A motion to dismiss.

Ms. GOLDBERG [continuing]. Saying, we're just a publishing platform. We're not a product. This is just speech. And then they attempt to get it dismissed. Oftentimes, judges will do it without even oral argument, and then we never get into discovery. So we never get the opportunity to even show or know exactly the extent to which the platform has been tolerating and making money off of this exact harm. We don't have any information about other similar incidents—nothing.

Senator WHITEHOUSE. So it's a vehicle not only for evading responsibility for bad acts, but it's a vehicle also for covering up what actually took place. It would be slightly different if the Section 230 dismissal motion was something that you made at trial, for instance—

Ms. GOLDBERG. Yes. And I—

Senator WHITEHOUSE [continuing]. So that you'd have a full chance, but they—not even that.

Ms. GOLDBERG. I also believe that even more terrifying to tech than facing a jury eye-to-eye is the discovery.

Senator WHITEHOUSE. Yes.

Ms. GOLDBERG. It was the discovery that made Omegle shut down. I had 60,000 documents showing all these other similar incidents of child sexual abuse, and they just—they shuttered their platform because they had no defense.

Senator WHITEHOUSE. Discovery is a beautiful thing. Senator Padilla.

Senator PADILLA. Thank you, Mr. Chair.

Mr. Guffey, I just want to begin with you and let you know that my heart goes out to you for you and your family's experience, and I really appreciate your willingness to be here today to share your testimony.

Representative GUFFEY. Thank you.

Senator PADILLA. I want to draw my colleagues' attention to what's represented to minors by a relatively new consumer product, character-based AI chatbot apps. Many of these services have been flooded with age-inappropriate chatbots which may cause young users to be exposed to sexual or suggestive AI-generated imagery or conversations. As a father of three school-aged children, this is personal. Further conversations with these chatbots can end tragically, as we've heard reports. Since 2023, at least two individuals have died by suicide following extensive conversations with AI chatbots. So the threat, colleagues, the risk is real.

Mr. Guffey, how would you recommend that this Committee begin to think about—or think through the risk posed by this emerging consumer product category?

Representative GUFFEY. Whenever it comes to AI, I would have to lean more on some of the other panelists up here on their expertise when addressing chatbots. Chatbots is something new that I have just started really looking into. But on the legal side, I'm not an attorney. So—I'm an angry parent that, you know, tries to throw it against the wall, whereas the attorneys are the ones who have to say, this is what will hold up in court, this is what will not.

Senator PADILLA. Well, we've had to figure out the legalese, but I do think you have the most important voice here, given your experience. I mean, the chatbot piece is just the next iteration—

Representative GUFFEY. Yes, sir.

Senator PADILLA [continuing]. Of this technology.

Representative GUFFEY. Yes, sir.

Senator PADILLA. We know what technology was when you and I were much younger—

Representative GUFFEY. Everything—

Senator PADILLA [continuing]. But what children have to contend with today, we can only imagine what's coming.

Representative GUFFEY. Well, and that's the exact problem. It's not just the problem—that's the problem of today, but it's as tech is evolving, our laws don't move fast enough to keep up with. And I believe that having that liability and being able to hold these companies responsible for what they are presenting—if we—instead of taking online services and treating it as a service, if we can simply treat it as a product, then we can hold them to consumer protection laws.

Mr. BALKAM. Senator, if I may, I think we should think about the international context in which this is playing out because the recent AI summit in Paris was called the AI Security Summit rather than the AI Safety Summit, which had taken place in the U.K. and, I believe, in Korea. And there's been a shift away from the prevailing thought that we must make these products safe, and instead—and particularly this administration is urging the vast and quick expansion of these tools. And I think you have a role, and

your colleagues have a role, to bring that focus back. And I dearly hope you do.

Senator PADILLA. Ms. Goldberg, you seem—

Ms. GOLDBERG. I do. One of my close friends, Matthew Bergman, is actually litigating a case against Character.AI where the bot encouraged addictive behavior and ultimately led the child to die by suicide. And I think what we'll find is that there's a possibility that courts will perceive this speech as the corporation's own speech, and in that case, Character.AI is owned by Google, and that it won't overcome a Section 230 challenge.

Senator PADILLA. Okay. Very good point, actually. So what I would do, just in the interest of time, is invite all of you to respond to the same question after the hearing as part of our questions for the record because I do want to get to at least one more topic. And I understand Senator Graham is on his way back, as well.

Last Congress, we had a hearing very similar to this, but instead of you five sitting in front of us testifying, it was actually the CEOs of the five largest social media companies testifying to the Committee. And I had the opportunity then to ask them each about the parental tools that they offer or didn't, but I think all of them offered some sort of parental tool to help parents—help minors safely navigate the use of their respective services.

I asked them to describe what those tools were, and more specifically what the adoption and use rates of those tools were because you can have tools and protections out there, and you can debate whether it's sufficient or not, but if people aren't even utilizing them, then kind of what's the point? And sadly, they either didn't share how widely used these tools were, didn't provide the data—and they're all very big into data—or what data they did show demonstrated to us that the usage rates were actually very low.

So the conclusion, unavoidable, undeniable, is that the industry isn't doing enough to let parents know what resources are available and aren't investing enough into understanding why these so-called protections aren't being adopted at greater rates.

Mr. BALKAM, in your testimony, you observed that these controls would better serve minors and their guardians if they were standardized, interoperable, and unified between apps, devices, and brands. How do you think we can make that a reality?

Mr. BALKAM. Well, I often use the example of the automobile industry. Back in the 1950s and 1960s, if you got out of one car and into another, you may not necessarily know where the blinkers are or the light switches were. Even the logos for those were different in different car makes. Well, laws came into place in the 1960s, and, in fact, now, when you get into a new rental car, you know exactly where the indicators are. You know exactly where the lights are. And the symbols are all the same.

Well, I'd like to see the industry come together, ideally voluntarily, but if not, perhaps with some coercion, to standardize the ways in which parental controls and online safety tools, which, by the way, are the ones that teens and young people use to stay private, to report, and to block, oftentimes without even their parents' knowledge. But in other words, let's have a standardized way of keeping our kids safe and that teens can keep themselves safe that is not as confusing as we got at the moment.

Senator PADILLA [presiding]. Yes, industry standards. It's not a new concept, and it tends to happen one of two ways. It either gets imposed by some level of government, and then industry comes away kicking and screaming, or they can actually live up to their responsibility and come together as an industry and put forward a model that is transparent and that either works or at least we can measure and hold them accountable when and where it doesn't.

I know it's been a long morning for all of you. Very, very much appreciate your participation in today's hearing and the work that you do and the perspectives that you've offered. I'm told Senator Graham is not coming after all, and so it falls upon me to not just thank all of our witnesses, but remind folks that the hearing record will remain open for 1 week for statements to be submitted into the record. Questions for the record may be submitted by Senators by 5 p.m. on Wednesday, February 26th.

And unless there's anything further from the nameplates——

[Laughter.]

Senator PADILLA [continuing]. This hearing is adjourned.

[Whereupon, at 12:26 p.m., the hearing was adjourned.]

[Additional material submitted for the record follows.]

United States Senate Committee on the Judiciary
Children's Safety in the Digital Era: Strengthening Protections and Addressing
Legal Gaps

Testimony of Stephen Balkam, CEO and Founder
Family Online Safety Institute

February 19, 2025

Good morning Chairman Grassley, Ranking Member Durbin, and distinguished members of the Committee.

My name is Stephen Balkam and I am the CEO and Founder of the Family Online Safety Institute (FOSI). FOSI is an international, non-profit organization whose mission is to make the online world safer for children and their families¹. FOSI convenes leaders in industry, government, academia, and the non-profit sectors to collaborate and innovate new solutions and policies that ensure a safer, more rewarding digital experience for all. Through research, resources, events, and special projects, FOSI promotes a culture of responsibility online and encourages a sense of digital citizenship for all.

FOSI has worked in this space for the past 18 years, but I have been involved in internet safety even longer, founding the Internet Content Rating Association (ICRA) and leading the Recreational Software Advisory Council (RSAC).

This is the third time I have testified before this committee. The first time was in 1995 at the dawn of the World Wide Web. During that hearing, I committed my organization to creating a content labelling system for websites so that parents could block the content they didn't want their kids to see. Thirty years later, we are working in a profoundly changed environment, though our values and mission remain the same.

¹ FOSI's homepage <https://www.fosi.org/>.

FOSI defines online safety as *acknowledging the risks, mitigating the harms while reaping the rewards of digital life*. This definition grounds our work by acknowledging that there are both positives and negatives that people of all ages experience on the internet.

In the “culture of responsibility” mentioned above, there is a role for all stakeholders to play to improve online safety: policymakers, law enforcement, industry, educators, parents and guardians, and the kids themselves.

FOSI works in the 3 Ps of online safety: enlightened public policy, industry best practices and Good Digital Parenting.

I am grateful for the opportunity to offer FOSI's perspective and expertise to the committee today.

Our recent online safety work can be summarized by the theme of our last Annual Conference: “From Protection to Empowerment.” This is not an either/or proposition - either we protect our kids or we empower them. It is a “both and more” concept that involves all of the stakeholders in the culture of responsibility. We want to protect kids *on* the internet, not *from* the internet.

We must shield our kids from the worst of the web, particularly younger children. There are parental controls of every shape and size, and it is unthinkable to offer a pre-K or elementary school aged child a device with unfettered access to the internet.

But beginning in the middle school years and certainly into high school, the training wheels start to come off. We as adults move from being helicopter parents to being more like co-pilots with our kids - working together to explore the best ways to use the online safety tools that social media platforms and apps have developed for young people.

From our own research, teens highly value the features that allow them to block, mute, report, or stay private². This agency, the ability to begin to take control of their digital experiences, is the beginning of the kind of independence and resilience we want to encourage in our teens and young people.

Empowerment can be the best form of protection. It's about preparing young people for the moment they step out into the world on their own, ready to face the best and worst of what the digital landscape has to offer.

Young people are citizens, and citizens have rights. We are bringing up the next generation of citizens who are, from a very early age, aware of and engaged in the online world. It is in all of our interests to ensure that these young citizens understand their rights and the awesome responsibilities that come with exercising those rights.

Bans of social media and phones have been proposed in various jurisdictions for teens under 16. Australia has even passed such a ban into law. Blanket bans deprive children from any positive experiences they may find online, are difficult to enforce, and open up too many possible unintended consequences.

Bans affect young people's rights to access content and participate online, which contradict both the US Supreme Court and the UN Committee on the Rights of the Child. Children have rights, including freedom of speech and access to information. Just because we are the only country in the world that has not ratified the UN Convention on the Rights of the Child does not mean that American children have no rights - only that they are being deprived in comparison to children around the world.

On the technical side, implementing a ban effectively remains a daunting challenge as no universal age assurance method has been agreed upon. Bans would also impact innovation by disincentivizing platforms from creating safety features for young users, incorrectly assuming that underage users will no longer be online.

² FOSI's Managing the Narrative: Young People's Use of Online Safety Tools
<https://www.fosi.org/policy-research/managing-the-narrative>.

What we need instead are thoughtful restrictions: ones that acknowledge the nuances of these issues, allow for flexibility at the local level or within the home, and feature the explicit involvement of young people themselves. The more we involve young people in the creation of thoughtful restrictions, the more they will buy into the rules that are eventually agreed. Bans handed down from on high will create a culture of mistrust and drive young people to find creative and far less safe ways around such laws.

Congress achieved great success when it passed the Children's Online Privacy Protection Act (COPPA). And the FTC has done well in the 25 years since COPPA's enactment, taking significant enforcement actions and issuing updates through the COPPA Rule³. But the law still needs to be updated or expanded upon.

What would be ideal is a federal privacy law covering adults and children alike. This could serve as the basis on which to build online safety legislation on top of. If there are already existing limitations on what data companies can collect and how it can be used, people will be more comfortable providing their personal information in exchange for safer online experiences, such as better online safety tools and age assurance processes.

COPPA effectively treats everyone under 13 as a child and everyone over 13 as an adult. Minors are not a monolith, to all be treated the same, but instead go through phases of development from birth through adulthood. As kids age, they develop more agency, more capabilities, more rights and more responsibilities. A simple binary of over/under 13, or even 18 for that matter, is insufficient in our modern age. Teens still deserve privacy (and safety) protections, but not necessarily identical ones to children under 13. The UK's Age Appropriate Design Code (AADC) does an effective job acknowledging children's different developmental stages, based in research and child psychology⁴.

³ FTC's Kids' Privacy (COPPA)

<https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/kids-privacy-coppa>.

⁴ UK's ICO AADC Annex B: Age and developmental stages

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/annex-b-age-and-developmental-stages/>.

Congress also did well to pass the Children and Media Research Advancement Act (CAMRA) in 2022 and funded it for the past two years. This essential and timely research into the impact of digital technology on children's physical and emotional development is exactly what the US government should continue funding, and results from the studies should serve as the foundation of evidence-based online safety policy.

The previous administration took a significant step forward in setting up the Kids Online Health and Safety (KOHS) Task Force⁵ through the National Telecommunications and Information Administration (NTIA) and Substance Abuse and Mental Health Services Administration (SAMHSA). The current administration should continue this important bipartisan work.

I was pleased to see the Senate pass the TAKE IT DOWN Act last week. That bill is a strong example of more targeted legislation that directly identifies and addresses a specific and important online safety issue. We hope to work with the House to see that legislation enacted.

The Kids Off Social Media Act is another example of promising legislation that could be effective in its goal. It is reasonable to want to keep children under 13 off of social media, and in most cases they are already excluded in platforms' terms of service. Getting the definitions correct is important, as we do not want to cut kids off from access to safe spaces that were built with their safety in mind, such as YouTube Kids, Minecraft, Roblox, and educational spaces like Wikipedia.

An additional section of this bill addresses algorithmic or personalized recommendation systems for children and teens. This is another worthwhile area for Congress to explore, and lawmakers should learn from the related laws passed last year in New York and California. I have some concerns about Title II of the bill, as I want to ensure realistic protections for kids on school devices and networks without

⁵ KOHS Task Force Recommendations and Best Practices for Safe Internet Use
<https://www.ntia.gov/press-release/2024/kids-online-health-and-safety-task-force-announces-recommendations-and-best-practices-safe-internet>.

imposing surveillance requirements or threatening essential funding for schools and students.

I am not a privacy or free speech absolutist. Of course privacy and free speech are important, protected rights. However, in order to pass effective online safety laws, I believe that there are opportunities for realistic compromises to be made. I expand on this more in the age assurance section below, but there are instances where it is reasonable for adults to give up a little privacy in order to access particularly harmful content or spaces online. I believe we can find a middle ground where young people have online safety protections while still maintaining a degree of privacy and access to consume and publish speech, and I am committed to working with Congress to achieve it.

Age assurance has become an integral part of the online safety policy discussions. We define age assurance as a broad term that describes various methods to discern the age or age-range of an online user including age verification, age estimation, and age gating. FOSI has conducted original research into age assurance in 2022⁶, as well as a white paper after a year's long working group in 2023⁷.

Age assurance is not a silver bullet that will solve all online safety concerns. However, it is a powerful tool that can be utilized to improve online safety, especially when thoughtfully considering the tradeoffs and use cases relating to proportionality. We present the tradeoff as that of invasiveness versus effectiveness - that is, to know a user's age with a higher level of certainty will almost always require more personal information. For online experiences that present relatively low risk to young people, it may be perfectly appropriate to use less precise age assurance mechanisms in order to access those experiences. Whereas for the most dangerous experiences or to access clearly harmful content, it would be justified to require a higher level of certainty and full age verification.

⁶ FOSI's Making Sense of Age Assurance: Enabling Safer Online Experiences
<https://www.fosi.org/policy-research/making-sense-of-age-assurance-enabling-safer-online-experiences>.

⁷ FOSI's Coming to Terms with Age Assurance
<https://www.fosi.org/policy-research/coming-to-terms-with-age-assurance>.

With technological advances, we believe that commercially feasible, privacy preserving age assurance is possible and will become even more effective through continued innovation in this space. Successfully incorporating age assurance measures into online safety laws will require risk-based proportionality, thoughtfully considering tradeoffs, and not being overly prescriptive with the technology or methods of assurance.

An alternative online safety perspective is safety by design. Discussing and legislating content moderation has devolved into debating what is actually harmful to kids, cherry picking examples of successes and failures, and legitimate concerns about violating freedom of speech and expression rights. Advancing the conversation to focus on a higher level of baseline protections offered to young users (raising the floor) is a worthwhile progression of the online safety policy discourse.

Australia's innovative eSafety Commissioner has been working on safety by design for years and has produced thoughtful guidance for industry to implement and governments to replicate⁸. The UK has also begun some of this work through its AADC. While it must be acknowledged that their AADC is based in privacy law and is specifically focused on data privacy practices, it still has an impact on children's online safety as its core requirement for industry is to consider and design for the youngest users, thinking critically through multiple stages of child development. We can learn a lot from the successes international regulators have had, and how to benefit from them here in the US while respecting our robust free speech protections.

While considering international approaches to online safety regulation, it becomes clear that the US is falling behind. In addition to the UK's AADC, which has been in effect since 2020, the UK has the Online Safety Act (OSA) which passed in 2023. The EU has the Digital Services Act (DSA), and Australia has its own Online Safety Act and an expert regulator in the eSafety Commissioner. While none of these regulations are perfect, they demonstrate multiple paths to improving online safety. Congress should learn from these creative ideas and improve upon them so that Americans of all ages, especially children and teens, are not left behind by their peers abroad.

⁸ eSafety Commissioner Safety by Design <https://www.esafety.gov.au/industry/safety-by-design>.

I also want to highlight the work of the Global Online Safety Regulators Network⁹ (GOSRN), a forum for independent regulators to exchange best practices and research across their jurisdictions. Current members include online safety officials from the UK, Australia, Fiji, France, Ireland, Republic of Korea, Slovakia, South Africa, and the Netherlands. I agree with the KOHS Task Force recommendation that the US, by way of the FTC, join the GOSRN as an observer until we have an effective online safety law and empowered regulator.

US states have begun to act on their own, with dozens of examples of online safety bills being introduced to require age-appropriate design, assert parental rights and permissions, require age verification, dictate content moderation, prevent addictive algorithms and targeted advertising, protect child influencers, and more. Unfortunately we have seen that most of these ideas, even if they pass into law, are swiftly challenged in court and blocked from going into effect. While the states are the laboratories of democracy and have offered some thoughtful and innovative solutions, there are significant contradictions between policies and concerns about regulating the internet differently across state borders. There is a role for Congress to play here, ideally setting a high floor of baseline online safety protections that states can build on top of if they choose.

Industry has a significant role to play here as well. Companies can and must do better to create easy to find and easy to use controls for parents and online safety tools for teens and young people. Apps and platforms need to do better to publicize and promote these controls and tools. And industry as a whole must better collaborate with each other - harmonizing tools across the ecosystem so that parents and teens are not overwhelmed with the task of setting and managing controls across countless apps, games, websites, and social media platforms.

Parental controls would be more effective and more utilized if they were standardized, interoperable, and unified between apps, devices, and brands. This is an opportunity for industry to work with lawmakers to improve the online safety experience for all families.

⁹ Global Online Safety Regulators Network, Ofcom
<https://www.ofcom.org.uk/about-ofcom/international-work/gosrn/>.

While FOSI primarily works with online safety issues that are harmful but legal (awful but lawful), I must acknowledge that there are some severe risks and harms to young people being online. When it comes to illegal content and action such as child sexual exploitation, human trafficking, and sextortion, we defer to our friends at NCMEC, Thorn, and law enforcement (including the DOJ and FBI) who have direct expertise and do excellent work in these disturbing areas.

However, FOSI can still be helpful in this space, serving as an upstream intervention with our preventative work. If our Good Digital Parenting resources¹⁰ are used effectively, they can help curtail kids from getting into positions where they can be exploited. The goal of our resources is to improve online safety conversations and restrictions as a family: more frequent, more informed and educated, more specific, more trusting discussions so that if a child encounters anything uncomfortable online (including the beginning of being groomed by a predator), they can bring their concerns to their family without fear of punishment or overreaction, successfully cutting off access to harmful content and conversations before the situation escalates. We have free resources available to facilitate these family conversations and restrictions, as does the US government thanks to the KOHS Task Force report¹¹ from last year.

This is also an opportunity to raise the importance of digital media literacy at home and in schools. Our friends at the National Association for Media Literacy, My Digital Tat2, Common Sense Media, and MediaSmarts have excellent resources for educators, and policymakers interested in improving media literacy education across the country.

FOSI's latest research report "Promoting Wellbeing in a Digital World"¹² from December 2024 offered a quantitative and qualitative look into teens' wellbeing. We

¹⁰ FOSI's Good Digital Parenting Resources

<https://www.fosi.org/good-digital-parenting-resource/resources>.

¹¹ KOHS Task Force Report Best Practices and Resources for Parents and Caregivers

<https://www.ntia.gov/report/2024/kids-online-health-and-safety/online-health-and-safety-for-children-and-youth/taskforce-guidance/best-practices-resources-for-parents-caregivers>.

¹² FOSI's Promoting Wellbeing in a Digital World

<https://www.fosi.org/policy-research/promoting-wellbeing-in-a-digital-world>.

released a subsequent analysis¹³ to highlight some key findings that could help inform policymakers in producing effective, nuanced regulation. Our top takeaways should not be surprising because they are outlined elsewhere in my testimony: think beyond bans; continue to fund research; and listen to the experts. I would also like to point out a couple more specific findings and related recommendations.

One is that definitions matter: lawmakers should carefully consider which services and platforms they intend to include in specific legislation. There are a variety of types of online spaces and platforms, and each may be used in distinct ways, with different purposes, risks, rewards, and impacts on digital wellbeing. Legislation that makes sense for social media platforms may be ill-suited to regulate gaming companies, streaming services, and possibly even adjacent spaces like livestreaming and discussion platforms. Some legislation takes a more thoughtful approach to definitions and scope than others. A possible path forward may be crafting narrower, more targeted online safety legislation that is focused on one sector or one aspect of being online.

I would be remiss if I did not also acknowledge that there are also significant benefits of digital experiences to teens' wellbeing. Both parents and teens reported that connecting with peers and learning new skills are the top benefits from being online. These positives are important to remember as online experiences have been incorrectly compared to tobacco or alcohol, which decidedly have no benefits to teen wellbeing. Congress can keep these findings in mind in order to mitigate online risks and harms while empowering teens to reap the rewards of their digital lives.

Let us challenge ourselves to reimagine what online safety can look like - not just as a range of restrictions, but as a foundation for resilience, confidence, and opportunity. Let's move from fear to trust, from limits to possibility, and from protection to empowerment.

Thank you for your time this morning and I look forward to your questions.

¹³ FOSI's Policy Implications of FOSI's 'Promoting Wellbeing in a Digital World' Research <https://www.fosi.org/policy-research/policy-implications-of-fosis-promoting-wellbeing-in-a-digital-world-research>.

Questions for the Record from Senator Alex Padilla
Senate Judiciary Committee
“Children’s Safety in the Digital Era: Strengthening Protections and Addressing Legal Gaps”
February 19, 2025

Questions for Stephen Balkam

1. Children today interact with a relatively new consumer product, character-based AI chatbot apps. Many of these services have been flooded with age-inappropriate chatbots—which may expose young users to sexual or suggestive AI-generated imagery or conversations. Further, conversations with these chatbots can end tragically—since 2023, at least two individuals have died by suicide following extensive conversations with AI chatbots. How would you recommend this Committee think through and respond to the risks posed by this emerging consumer product category, given your experience with child online safety?

Thank you for your question, Senator. There are a couple of ways to think through this new technological risk to children’s safety.

The easiest place to start is with transparency and disclosure. There is a real benefit to having a visual warning that informs the user that the conversation they are having is not with another person or being who thinks like them. This is especially important for children, who are quick to anthropomorphize many things in their lives, let alone powerful technological systems built for excelling at human-sounding communication. Some type of warning or label, up front, constant, or periodically, should be used to remind users that a chatbot is technology and its side of the conversation may not be accurate. Transparency, disclosure, and warnings should be the bare minimum.

Some states have been quite active in this space, and a good summary of legislative efforts can be [found here](https://www.multistate.ai/updates/vol-46)¹. Your home state was the first to regulate chatbots with a clear and conspicuous disclosure that the interaction is with a bot. To quote the article, “disclosure laws are low-hanging fruit that offer lawmakers an opportunity to set some guardrails on AI technology without requiring onerous registration or reporting requirements.” As such, they should be a great first step for you and the committee to pursue.

¹ <https://www.multistate.ai/updates/vol-46>

Another option is to think about how this technology can be regulated more as a product than as speech. [California is also exploring](#)² this interesting legislative approach, aiming to protect kids by reducing the addictiveness of such a product.

Considering the chatbots as products also opens an opportunity for content moderation. If there are potentially harmful phrases entered related to death, suicide, self-harm, or severe loneliness, that should trigger some type of safety intervention that stops that train of thought or conversation. This could be an opportunity for the chatbot to provide medically approved and age-appropriate resources, as social media platforms have started to do. Legislation requiring content moderation has proved difficult for social media platforms because of the strong free speech protections in the First Amendment. But it is unlikely those same protections apply to an AI-powered chatbot.

Finally, I would like to reference my [written testimony](#)³ regarding age assurance and the best interest of a child. Building products with the youngest user in mind, with the highest safety settings on by default, should also help to address the harms raised by this technology. Perhaps the safest version of a chatbot is publicly available for anyone to use, but in order to discuss potentially harmful topics a user needs to go through some form of age assurance.

Thank you for the question and I am happy to discuss any of this further if it would be helpful to you or the Committee.

Sincerely,
Stephen Balkam
CEO & Founder, Family Online Safety Institute

² <https://www.politico.com/newsletters/digital-future-daily/2025/03/06/a-novel-idea-for-controlling-chatbots-00216736>

³ <https://www.judiciary.senate.gov/imo/media/doc/2025-02-19-testimony-balkam-1.pdf>

February 19, 2025

Written Testimony of Carrie Goldberg

Founder, C. A. Goldberg, PLLC

Before the U.S. Senate

Committee on the Judiciary

“Children’s Safety in the Digital Era: Strengthening Protections and Addressing Legal Gaps”

Chair Grassley, Ranking Member Durbin and distinguished members of the Senate Committee of the Judiciary.

My name is Carrie Goldberg. I’m a lawyer who represents families catastrophically injured by tech.

I stand for the belief that our courts are the great equalizer. And the people who’ve been injured should have access to the courts. No matter how big, rich, or omniscient the adversary.

I stand against the idea that some bad actors – whether human or corporate are too important to face their victims eye to eye, undergo discovery into how the horror happened, face the stare of a jury, or pay for their harms. Companies that mint money off the backs of the masses can’t later claim when their product hurts people – KIDS – in predictable – or even known ways -- that it’s not their fault, they’re just a passive publisher.

I want to tell you about a few of the cases I work on every day.

- The family of Bianca Devins from upstate NY who was 17 when her murder was live posted on Snap and Instagram; Instagram refused to remove the murderer’s profile as it went viral. and her family is harassed daily by people who defile her murder pictures. In her death, Instagram went from 2k to almost 200k and TO THIS DAY Meta refuses to give control of the account to her estate. To make matters worse, when the local prosecutor’s office in Oneida County distributed the murder videos and CSAM of Bianca to YouTubers and documentary makers, the Northern District of New York ruled that her estate did not have standing to bring claims under 2255 and 2252A for CSAM because the estate could not be injured from Bianca’s CSAM distribution. *Estate of Bianca Devins v. Oneida County, et al.* NDNY, 6:21-cv-00802 (2021)
- 11-year-old A.M. from Michigan who used Omegle after a slumber party. This website matches strangers for livestreaming. Omegle matched A.M. with one of the thousands of predators. For 3 years she became his online sex slave at the beckon call of he and his friends to perform sexually. Sometimes interrupting her at school

or the dinner table; even forcing her to go back on Omegle to recruit more kids. The abuse eventually ended when his home which he shared with his wife's daycare was raided and images of A.M. and other young girls were found. We overcame section 230 on our product liability and trafficking claims in the District of Oregon. In a settlement with A.M., Omegle shut down last November and declared bankruptcy.

- I'm the originating attorney in a case against Snap where our clients' children were matched with drug dealers and sold counterfeit fentanyl laced drugs that killed them. The case, which overcame Snap's demurrer, now has 90 families in it from all over this country – including families of 17 yo Daniel Puerta, 14 yo Alexander Neville and 19 yo Devin Norring.
- L.S. was 13 using the site, BandLab, which has no age restrictions, to livestream with a boy she thought was 17 but really was 40-year-old Noah Madrona a pedophile from Portland Oregon. He posted openly on the music sharing platform including songs called Pedophile in A Minor. On June 24, 2022, Madrona drove 15 hours to her home, abducted her on her way to school, stuffed her in the trunk of the car and raped and abused her for 8 days. While there was a national manhunt, Bandlab refused to provide law enforcement key information that could have led to her faster rescue because they wanted to respect Madrona's privacy.
- A class of children whose CSAM went viral on Snapchat as a result of criminals accessing a known security defect about which families were not warned of.
- John Doe, a 15 yo with profound Autism who got funneled into Grindr's marketing campaigns on TikTok and Instagram. In their social media posts they use children in PE class and other school settings. John Doe uploaded the product from the Appstore at school and over the next four days was recommended to adult men, four of whom raped him over four consecutive days. 3 were prosecuted. Grindr is a hookup app. And in court they said they had no duty to restrict children's access. On February 18, 2025, the 9th Circuit affirmed the district court, holding that Grindr was immune from liability for the non-trafficking claims because of Section 230, and saying John Doe did not show Grindr had actual knowledge of the trafficking despite John Doe pleading Grindr knew about the trafficking from repeated lawsuits, media articles, its own campaigns to children on social media, over 100 criminal cases, media articles, and a peer-reviewed study from the Journal of Adolescent Health finding that half of sexually active gay boys had their first sexual encounter with an adult they met on Grindr.
- The family of 16 yo Ayden Wallin from Colorado who in July 2020 discovered a website glorifying suicide and learned about a product he could get from Amazon which he used to end his life. In Sept 2020 Meredith Mitchell his mom exchanged 57 messages with Amazon. Amazon knew the product had no use besides suicide. And kept promoting, selling, and delivering it. I represent 27 other families in 9 (soon to be 10) cases in Washington State whose children bought the suicide chemical after Amazon sold it to Ayden.

In all my cases, Defendants raise two main defenses. Section 230 of course. But also that they didn't have specific or actual knowledge of my client or their abuser, their account, their picture. They did not *intend* to harm my client they claim.

I was here a year ago, on January 31, 2024 when this Committee questioned the CEOs of Meta, Twitter, Discord, Snap, and TikTok. You said you were done with discussions and desperate for solutions.

But the most important thing I can say as an attorney who represents victims of extreme harms online, is that details matter. We can't have solutions that swap in one obstacle for families with another. For instance, it just won't work if we remove Section 230 immunity, but replace it with the requirement that a plaintiff must plead the platform had actual knowledge of the specific incident of CSAM or trafficking.

I. ANALYSIS OF 2255A'S ACTUAL KNOWLEDGE STANDARD ON CIVIL CSAM LITIGATION

Currently, Section 2255(a)(2) of the proposed STOP CSAM ACT creates a civil remedy for victims of the "intentional or knowing hosting," "storing," or "making . . . available" of child sexual abuse material by an interactive computer service.

Exhibit A contains letters from victims whose justice would be curtailed by an actual knowledge standard. Some are people with pending litigation.

Section 2255A(f)(2) defines "knowing" as "knowledge of the instance when, or the course of conduct during which, the provider" "hosted," "stored," or "made available the CSAM "at issue."

This definition of "knowing" is known as the "actual knowledge" standard. The Actual Knowledge standard is the most stringent for a victim to plead. To prevail, a plaintiff must show a provider was "in fact. . . aware" of the specific incident.

Practically, an Actual Knowledge standard will make it almost certain that a victim's case will be thrown out at the earliest stage in litigation, a motion to dismiss. That's because of two reasons: 1) platforms historically have taken a head-in-the sand approach to harms that occur to victims. Platforms make it difficult to report, the reports go nowhere, victims don't get receipts, if a victim does report at what point does knowledge get imputed to the platform especially when they use AI? 2) asymmetry of information – it's only through discovery that a plaintiff is likely to learn the extent of a platform's knowledge, but a case will never get to discovery because it will be thrown out before that for failure to allege facts sufficient to show the platform had actual knowledge.

As the dissent in *M.H. v. Omegle* explained, 2255 actual knowledge for CSAM cases is not necessary. In *Tilton v. Playboy* (11th Cir 2009), the knowledge element can be demonstrated through actual knowledge OR deliberate ignorance. Knowledge through deliberate indifference occurs when a party acts "with an awareness of the high probability of the existence of the fact in question." (*US v. Hristov*, 11th Cir. 2006). This "deliberate indifference" rule exists to prevent a party who has had his "suspicion aroused but then deliberately omits to make further enquiries [] because he wishes to remain in ignorance" from "skirting liability" *Id.*

Where courts have applied actual knowledge standards, victims have lost:

- *Doe v. Twitter*, N.D.Cal Dec 11, 2023 Involved the CSAM of two minor boys. John Doe #1 provided evidence that Twitter knew the victims were underage, reported the video to Twitter, stated he was a minor, showed his driver's license, showed that his mother submitted two previous complaint. **Despite this mountain of evidence**, the court said this was not enough to prove "actual knowledge" and instead amounted to "turning a blind eye" rather than active participating in sex trafficking.
- *M.H. v. Omegle, LLC* the 11th Circuit found there was no actual knowledge despite extensive pleadings that on Omegle the use of the website for advertising, creating, posting and sharing child sexual abuse material was so pervasive" as to be the actual business model.
- *Does v. Reddit*, the 9th Circuit said there was no actual knowledge despite evidence that Reddit had received reports of the CSAM.
- In *Doe v. Grindr* the plaintiff pleaded that Grindr actively advertised to children on Instagram and TikTok using child models at school settings. The pleadings exhaustively explained Grindr's knowledge of its trafficking to children -- prior criminal and civil cases involving them recommending children to adults for in-person sex, media articles about the sexual abuse of children, and a peer-reviewed article in the Journal of Adolescent Health that found that 50% of sexually active gay children have their first sexual encounter with an adult they met on Grindr. On February 18, 2025, the 9th Circuit affirmed the district court saying, Grindr's knowledge was too attenuated.

In no other type of case is the standard so high. Such a high standard just provides a new benefit to tech platforms.

If the breaks of a car go out, a beam falls on somebody's head in a construction zone, or a door flies off a plane, the injured people don't have to prove the defendant had actual knowledge of the problem beforehand and intended for the injury to occur to the exact person.

Cases where victims have overcome Motions to Dismiss without importing this Actual Knowledge standard from criminal law:

- *AM v. Omegle* in the District of Oregon for product liability relating to the defective design and failure to warn inherent in matching adults and children for sex streaming
- *AM v. Omegle* relating to Omegle's knowledge that it was operating a trafficking venture in that it knowingly recruited children and made money of the scheme
- 5 cases against Amazon for selling suicide chemicals even though they claimed not to have the intent for the decedents to ingest the chemical
- *Neville v. Snap* -- Cases against Snap for operating as a cartel for counterfeit fentanyl pills
- *A.B. v. Salesforce* -- Plaintiffs allege that Salesforce enabled Backpage to process credit cards, text potential and past clients, and gather information about sex

traffickers. Plaintiffs' case overall rested on the notion that Salesforce provided back-office business services to a company "it knew or should have known was engaged in sex trafficking." On December 19, 2024 the Fifth Circuit ruled for Plaintiffs, affirming the district court's denial of summary judgment and remanding the case to trial court.

- *Doe v. MG Freesites, LTD* – On December 19, 2024 the Northern District of Alabama Western Division ruled in favor of plaintiffs, denying Pornhub's motion for summary judgment on claims relating to trafficking and CSAM. Plaintiffs pleaded that Pornhub's algorithm and system of reviewing, categorizing, tagging, and disseminating images and videos depicting the rape of minors satisfied the pleading standard. Defendants use their algorithm both to help users find CSAM and helped users advertising CSAM to advertise it.

II. **ESSENTIAL FACTORS IF THE TRUE GOAL IS TO PROTECT CHILD VICTIMS FROM ONLINE EXPLOITATION**

The following propositions are anti-victim and no properly counseled victim will ever support legislation with this language:

- Creating an "actual knowledge" standard in civil causes of action. As discussed already, the actual knowledge standard is one imported from criminal law and almost never is used in civil cases. The proper standard is negligence. The compromise is recklessness where the defendant knew or should have known they were creating a risk. It makes sense to have a higher standard in criminal law where due process supports the notion that people should only be criminally liable for intentional conduct. That standard does not work in civil cases where the purpose is to make injured people whole for harm where somebody negligently or recklessly caused their harm or whose affirmative conduct increased the likelihood of harm.
- Sanctions. Sanctions standards are already set in state and federal rules of civil procedure. Establishing new more lax standards will encourage bullying by big tech during litigation. Already Snap has a pattern and practice of filing frivolous sanctions motions against victims and their attorneys with demands that plaintiffs change their pleadings. For instance, on September 25, 2023, Snap, an \$18b company moved to sanction my clients, grieving parents of children who died from their product connecting them with drug dealers, and me. Why? Because we had the audacity to sue them – claiming they failed to cooperate with law enforcement and their features facilitated drug deals – Quick Add, Snap May and My Eyes Only. We won the motion to dismiss for this complaint they alleged was frivolous and are now in discovery. Our research in defending this motion revealed Snap usually files sanctions motions against victims. Lee Davis is forced to defend a sanctions motion by Snap. Most attorneys never move for sanctions in their entire career. Snap does it at the beginning of almost every lawsuit just to intimidate and bully victims.
- "Impossibility" defense. No law relating to trafficking or CSAM should have a defense where platforms can say it is technologically impossible to disable access to or remove CSAM or stop trafficking. If a platform does not have the technology

to remove CSAM or stop abusive accounts, it is an inherently dangerous product and should not be in the stream of commerce for American people. Period.

III. WHY GETTING TO DISCOVERY IS KEY

Discovery puts parties on equal footing because the facts of the case are laid bare for both parties. This puts parties on equal footing to evaluate the strengths and weaknesses of the case. The purpose of discovery is to ensure both parties have access to all facts surrounding their dispute so they can make informed decisions during trial proceedings.

The trouble is that discovery only happens when parties are on the other side of a motion to dismiss. In cases where a case is dismissed on grounds of Section 230 or lack of actual notice to the platform, the case never gets to discovery. This deprives the victims of key facts that they need at the pleading stage to win a motion to dismiss. So it's a Catch – 22 for victims: because their case is dismissed for lack of specific facts in their pleadings about the platforms, they don't get to advance into discovery to collect those facts. The end result is that platforms can continue to harm so long as they never get to discovery where it would be revealed.

Discovery is particularly important in cases where there is asymmetry of information as in cases against corporations relating to products. Here our defendants are social media companies with more data than we can imagine. They hold all the cards about how their products work, the extent of their knowledge, prior similar incidents, the intentionality of the design that led to the injury, whether things were reported, prior misuse by the offender

For many grieving parents, discovery IS the point of litigation because they want to . They want the harm to never happen to another family. Discovery is where transparency happens. It's far more threatening to tech companies than money damages.

In one rare case that advance into discovery, *A.M. v. Omegle*, in the district of Oregon we obtained about 60,000 documents of discovery from Omegle. And right as I was taking depositions, Omegle folded, shuttered their website in November 8, 2023 and declared bankruptcy. Their RIP website page now says "I thank A.M. for opening my eyes to the human cost of Omegle." Interestingly On December 19, 2023 – just one month after Omegle shutdown, I received an offer from a "nonprofit" called Tech Coalition that is actually run by the executives of TikTok, Meta, Google, Amazon, Microsoft, and Roblox. They asked to buy my Omegle discovery to train their AI but only if I signed an NDA. I said I'd give it to them free and they weren't interested. I also pointed out that the only reason I had the discovery was because I won the motion to dismiss twice – which is something their coalition members always plead

[Case studies of matters dismissed under Section 230](#)

IV. SOME OF MY CASES DISMISSED UNDER SECTION 230

A. Immunity for distributing suicide kits

McCarthy, et al., v. Amazon.com (Pending in the 9th Circuit)

In February 2021, I was hired by Ruth Scott. Two months prior, her only child, Mikael, had discovered a pro-suicide website where people could encourage each other to die and they could live-post it. Users on the site recommended a specific chemical for sale on Amazon, Sodium Nitrite, that was only twenty dollars, and ensured a fast death delivered to your doorstep. Indeed, a teaspoon of the powder mixed with water ends a life in about 20 minutes. On Amazon's website I saw pictures of the product and lots of user reviews from heartbroken parents and toxicologists saying the product had killed their kid.

I expected the case to just be a pro bono letter. Surely Amazon was just too big to realize it was selling a suicide kit. And I say kit, because it recommended that users who purchase the chemical also buy attending products to guarantee death – including a small scale to measure the dose, Tagamet anti-emetic pills to prevent vomiting, and an Amazon edition suicide manual with an entire chapter on how to die from Sodium Nitrite. Mikael had also the scale and Tagamet was found in his room.

Unlike the other products Amazon sells, the 99% pure Sodium Nitrite it sold to Mikael has no household use. [Contrast to curing salts which are 6% pure and dyed pink for safety because even that purity is dangerous].

To my surprise, when Amazon's lawyers responded in May, rather than taking the product off the market, they doubled down and said they have no duty to restrict sales just because somebody was "misusing." They said they could not be held liable anyway.

I ended up suing Amazon. And other parents joined the fight. I now represent 24 families to whom Amazon knowingly sold this chemical. We have six cases filed. One of the cases is on behalf of the families of a 16 year old girl, Kristine Jónsson from Ohio and 17 year old Ethan McCarthy from West Virginia

In that case, I sued saying that Amazon was negligent for selling and distributing Sodium Nitrite when it knew that the product was regularly used for death. I explained in the long pleadings all the different sources of Amazon's knowledge that it was selling the chemical – including it receiving a letter from Congress demanding answers. I explained that Amazon removed one-star reviews to manipulate the ranking of the product and suppressed the warnings that parents left.

The lawsuit sues Amazon for its role as a seller – not as a platform. It was a basic seller negligence case. But the judge said that since I had mentioned user reviews – i.e. content posted by another user, Section 230 applied and the claim should be thrown out. This was one sentence in a 42 page complaint and none of the claims even relied on that fact. The Court dismissed the case with prejudice and said Amazon was immune from liability for intentionally concealing the harms connected to the product because the lawsuit included language that discussed the posting of third party content.

B. Immunity for marketing a hook-up app to children

John Doe v. Grindr (dismissed with prejudice, 9th Circuit)

Grindr is the world's biggest hook-up app for LGBTQ+ individuals. In recent years, it has begun campaigns on TikTok and Instagram clearly marketed to children. Not only are these platforms primarily used by children, but the content Grindr posted showed videos of adolescent-appearing kids in school gymnasiums and high school or middle school settings.

In April, 2019, John Doe, a closeted 15 year old gay boy living with Autism and ADHD in a rural community fell victim to Grindr's juvenile-targeting marketing. He was desperate to meet other gay kids and naively thought he could find friends on Grindr. Without his parent's knowledge or permission, he downloaded the app, complied with a prompt that told him he needed to be 18 or older and created a profile, choosing whatever birthday he wanted. Grindr extracted John Doe's location data from his phone and offered proximately located users to him and offered him to nearby adults. The day he downloaded Grindr, he matched with an adult nearby his school, met up with him and was raped. Stunned, traumatized, and confused, Doe returned to Grindr. Over four consecutive days in total, Grindr matched Doe with four adults, each who raped him with varying degrees of force and violence. Three of the four were criminally convicted. Doe experienced significant trauma and distress from the rapes, causing him to attempt suicide, drop out of school, and require inpatient hospitalization.

On March 10, 2023, Doe sued Grindr under theories of strict products liability, negligence, and trafficking. He alleged that Grindr breached its duty of care by aggressively marketing to children and then matching them with adults. Grindr alleged that it is but a forum for "speech." The District Court dismissed the entire case with prejudice, claiming that but-for the user content, none of the harms that befell Doe would have occurred. The judge lamented that "[t]he facts of this case are indisputably alarming and tragic. No one should endure what Plaintiff has." Yet, he dismissed the case because, according to the Court, Section 230 immunizes the platform because if not for user content – specifically the location data Grindr extracts from users to match them with other users – none of the harms would have happened to Doe. The trafficking claims were dismissed because the judge said that Grindr merely "turned a blind eye" to the unlawful conduct, which it is allowed to do. On February 18, 2025 (one day before this hearing) the Ninth Circuit ruled against my client affirming the lower courts dismissal. Next stop is to petition the Supreme Court of the United States to hear this case, making it the court's first substantive decision on Section 230.

C. Immunity for Extreme Stalking the Platform Knew About

Matthew Herrick v. Grindr (dismissed with prejudice, 2nd Circuit)

Starting in October 2016, 33-year-old Matthew Herrick began receiving unwanted strangers at his home and work. Sometimes as many as 33 in a day. Matthew knew his ex was behind the strangers – they began showing up a week after their break-up. The

impersonating profiles sent men for fisting, orgies and aggressive sex. In the direct messages, the strangers were told that Matt's resistance was part of the fantasy. Matthew had tried everything he could to take care of the problem on his own. He filed more than a dozen complaints with his local police precinct.

In all, about 50 separate complaints were made to the company reporting the fake profiles, either by Matthew or on his behalf. The only response the company ever sent was an automatically generated email: "Thank you for your report." Over the course of ten months more than 1,400 men, came to his home and workplace expecting sex.

Even though Grindr's terms of service state that Grindr can remove any profile and deny anybody the use of their product at the company's discretion, they refused to help. After Matthew's approximately 50 pleas to Grindr for help were ignored, we sued Grindr in New York State Supreme Court, New York County, and obtained immediate injunctive relief requiring that Grindr ban the malicious user.

It's not clear exactly how Grindr was so easily being used to send the strangers to Matthew—it might have been through a spoofing app that worked with Grindr's geolocation software or something more technical. But the strangers who came to Matthew said they were sent through the Grindr app and would show Matthew the fake profiles with his pictures, geolocation maps showing how far away they were from Matthew, and direct messages telling them which buzzer to ring and what kind of sex Matthew was eager to have.

We sued Grindr under product liability theories. Grindr is a defectively designed and manufactured product insofar as it was easily exploited—presumably by spoofing apps available from Google and Apple—and didn't have the ability, according to the courtroom admissions of Grindr's own lawyers, to identify and exclude abusive users. For a company that served millions of people globally and used geolocating technology to direct those people into offline encounters, it was an arithmetic certainty that at least some of the time the product would be used by abusers, stalkers, predators and rapists. Failing to manufacture the product with safeguards for those inevitabilities, I argued, was negligent.

The SDNY judge dismissed the claim with prejudice declaring that Grindr was immune from liability pursuant to the Communications Decency Act, because according to her, our claims depended on information provided by another information content provider. If not for Matthew's ex using the app, she reasoned, none of this would have happened to Matthew. She reduced all the harm as flowing from the ex's actions, not Grindr's, and therefore reasoned that the company was immune from liability and had no obligation to Matthew.

We appealed to the Second Circuit repeating the argument that because we were suing Grindr for its own product defects, operational failures and broken promises in their terms of service—and not for any content provided by Matthew's ex—Grindr was not eligible to seek safe harbor from Section 230. To rule against Matthew would set a dangerous precedent, establishing that as long as a tech company's product was turned to

malicious purposes by a user, no matter how foreseeable the malicious use, that tech company was beyond the reach of the law and tort system.

On March 27, 2019 the Second Circuit issued a [summary order](#) affirming the district court's dismissal of the complaint. On April 11, we filed a petition for panel rehearing, or, in the alternative, for rehearing *en banc*. On May 9, that too was denied. In October 2019, our writ for certiorari to the Supreme Court, also was denied. It was the end of the road for *Herrick v Grindr*.

In 2020 Justice Clarence Thomas wrote a dissent to a writ for certiorari in the case *Malware Bytes, Inc. v. Enigma Software Group*. He lamented that when Congress enacted Section 230, most of today's major Internet platforms did not exist. Then he condemned how the two and a half decades of lower court decision "eviscerated the narrow liability shield" Congress had intended. Making his point, he cited Matthew's case, furious that courts so extravagantly interpreted Section 230 that it even granted immunity in a product liability case "concerning a dating application that allegedly lacked basic safety features to prevent harassment and impersonation."

IV. CONCLUSION

What is illegal online, should be illegal offline. Americans are being injured by tech companies running amuck, unconstrained by regulation, liability for their product, or the threat of litigation. Everyday people lost their fundamental right to the courts to vindicate their injuries because of Section 230. In fixing it, Congress must use care to not pass so-called protections that would do more harm than good. For instance, creating an "actual knowledge" pleading standard would be even more deadly to cases than Section 230 is. Court will be even more unfriendly to victims if new laws provide lax rules for defendants to sanction victims and new defenses for platforms to claim a fix is "impossible." When Congress passed Section 230, it never imagined what the Internet would become or the complexity of future products. Now it knows it birthed a monster. Through careful legislative reform, Congress can fix what corporations won't because of greed and courts can't because of bad accumulated case law. Anybody could become my next client.

EXHIBIT A

Dear Senators,

I go by A.M. to protect my identity as I stand up against what has happened to me and so many others. I would appreciate your time to hear my story as I urge you to reconsider the STOP CSAM Act.

While living in Michigan at the age of eleven, I went on to Omegle expecting a site designed for people to meet others. Within an instant, I met my abuser who then spent years sexually coercing me with the threat of killing my family. Faced with fear, I spent years silently being torn apart. This was not one instance, but countless messages, photos, and videos I was forced to hand over. Even being sent back to Omegle in an attempt for my abuser to use me as bait to find other underage girls.

Due to this abuse, my family and myself have suffered immensely. I have faced severe PTSD, unable to even hear a phone ringing without having a panic attack. I am constantly flooded with flashbacks that can cause such distress that I have seizures to try and stop the memory. Forever having to explain to others pieces of what I went through so they can understand the nightmares, or the seizures, or the strains within my family system.

The horrors I faced are unrepeatable. The list of ways this has impacted me is miles long. It forced me to have to publicly come out with my abuse and allow it to be used as an example of the dangers of this site and so many others. Placing myself at the mercy of the court system and the public eye in order to have a chance at protecting other young people like me.

If I had to plead that Omegle knew about my specific abuse at the time it happened, my case would have been thrown out for that reason alone, even if I had won on Section 230 grounds. As a direct result of my case, Omegle has been shut down forever. This means that no child will face what I faced. Yet, this was only possible after I obtained over 60,000 pieces of evidence in the discovery time of my legal battle. That is 60,000 children who faced abuse like mine. 60,000 pieces of evidence that would have stayed unearthed had we continued to let tech companies hide behind their ignorance.

STOP CSAM as drafted with an 'actual knowledge' standard will allow tech companies to hide behind a defense of claiming that they lacked "actual knowledge"

of victims' CSAM or trafficking. It is impossible for a victim or parent to be able to provide that information to a lawyer prior to the filing of the lawsuit. The requisite information resides with the technology companies who knowingly turn a blind eye and who intentionally hide from wanting to know what their platforms are facilitating. Please do not hand them another shield. Children's lives are at stake.

I spent years being tortured. I endured emotional and sexual abuse that will forever impact my life. I will never forget what happened to me. I will never be able to walk away from it. I will never, ever, get my childhood back. I am urging you to please remember me when you make these decisions. Not as the woman I was forced to become, but as the child that could have been saved.

Sincerely,

A.M.

Mother of J
31 Hudson Yards, 11th Fl
New York, NY 10001
February 17, 2025

Chairman Senator Chuck Grassley
135 Hart Senate Office Building
Washington, DC 20510
Ranking Member Senator Dick Durbin
711 Hart Senate Office Building
Washington, DC 20510

Chairman Senator Chuck Grassley
135 Hart Senate Office Building
Washington, DC 20510
Ranking Member Senator Dick Durbin
711 Hart Senate Office Building
Washington, DC 20510

Re: STOP CSAM

Dear Senator Grassley and Senator Durbin:

My name cant be shared to protect my daughter. I am the mother of a CSAM survivor who was abused from days after she got home from the hospital until she was a toddler, and is revictimized every day since as her images recirculate on tech platforms.

This bill, asking tech prove actual knowledge of each image before asking them to clean up their own mess makes a mockery of my daughter's efforts to seek justice. If this bill is all we can pass in the tech controlled political environment we live in now, then do nothing. It's that simple, if you won't help us than at least don't hurt us. Thank you.

Sincerely,
Mother of J

"Amy" of the Misty Series
31 Hudson Yards, 11th Fl
New York, NY 10001
February 17, 2025

Chairman Senator Chuck Grassley
135 Hart Senate Office Building
Washington, DC 20510
Ranking Member Senator Dick Durbin
711 Hart Senate Office Building
Washington, DC 20510

Chairman Senator Chuck Grassley
135 Hart Senate Office Building
Washington, DC 20510
Ranking Member Senator Dick Durbin
711 Hart Senate Office Building
Washington, DC 20510

Re: STOP CSAM

Dear Senator Grassley and Senator Durbin:

The STOP CSAM act has been a reoccurring problem for survivors of this offense and the fact that tech companies support this bill should be the first red flag. This bill is not aptly named. My lawyers are finally making progress to hold tech to account in courts, and I am so worried that the tech industry is planning to impose this heavy burden on survivors and their lawyers before accessing justice. Please take the words of survivors to heart and let's pass a bill that helps seek real justice.

Sincerely,

"Amy" of the Misty Series

"Erika" sister of "Tori"
31 Hudson Yards, 11th Fl
New York, NY 10001
February 17, 2025

Chairman Senator Chuck Grassley
135 Hart Senate Office Building
Washington, DC 20510
Ranking Member Senator Dick Durbin
711 Hart Senate Office Building
Washington, DC 20510

Chairman Senator Chuck Grassley
135 Hart Senate Office Building
Washington, DC 20510
Ranking Member Senator Dick Durbin
711 Hart Senate Office Building
Washington, DC 20510

Re: STOP CSAM

Dear Senator Grassley and Senator Durbin:

This is a pseudonym I have to use for my own safety. My little sister and I wrote to congress together a few years ago to pass the no time limit for justice act. She was the strongest person I know, and she would have never wanted to write you this letter. She would say: Why do victims have to bear the burden of fixing the problems that made us victims? Why did I come here and bear my soul just to beg you to do what is right. She felt we had been through so much that we do not owe this to anyone. But I owe this to her. She isn't here to fight for herself or fight for justice in any way anymore.

We were both victims of child sexual abuse that was memorialized by our first abuser and shared with the world online. Our offline abuse was being captured and shared in a virtual web of pedophiles. One of the second-hand abusers wanted to meet us offline. He became obsessed with us and wanted to make the pictures he saw of us a reality. We were brought from the state we lived in to a hotel to meet this monster multiple times. It was a miserable circle of abuse no kid should ever be put through.

I think back to when she was this sweet beautiful little kid. Her childhood was stolen, captured, and put online for the sick fantasies of pedophiles. Her exploitation was immortalized. What happened to us really couldn't have ever happened without big tech—and big tech will continue to let this run rampant if we do not take action. If you pass STOP CSAM, which is supported by Tech companies like Snap and X and Google, then you will be letting me and my sister down.

What I can't really understand is why you would not pass a bill that will actually help us. Even though she is gone, her online abuse continues forever. This abuse is permanent even though we are not. These digital crimes have outlived my sister.

Right now, there is no way to seek criminal restitution or civil justice after the victim dies. Copyright holders have more rights than that. Big tech treats copyright holders better than victims. And that is why Congress needs to step up and pass real reform instead of STOP CSAM which has such a high burden no victim will be able to seek justice. It's time to do something to start protecting children living and dead, known and unknown.

We need to expand the rights of survivors and limit the rights of tech companies. That is why I came here today. I am here to ask you to hold tech to account for real. Please heed the echoing call to help survivors like myself before it is too late.

Sincerely,
"Erika" sister of "Tori"

February 18, 2025

Dear Senators:

My name is Mrs. M. Smith, and I am a Canadian citizen writing you today to represent the astronomical and increasing number of victims that have been subjected to online harm. Allow me to share with you the story of my daughter's abuse.

At the age of 12, my daughter had a cell phone, which we ensured was equipped with parental controls. She was not on social media at all, her screen time was limited, her contacts needed to be approved, and her father could see all of the activity on her phone. Therefore, it was shocking to us to learn that our daughter, at the age of 12, could be groomed and manipulated online on a school device, which carried the music platform, Bandlab. This platform does not have any age restrictions, and it has a chat function like many. This platform was evidently not monitored adequately by the tech provider, specifically for CSAM, to detect the online predator she was speaking with. For one year, an online predator, who presented himself as a peer, groomed her and published sexually explicit material of our daughter online. In June of 2022, at the age of 13, the predator, a 40-year old man, named Noah Madrano, abducted my daughter right beside her school.

When my daughter did not arrive home on the school bus, I reported her as a missing child. From there, a full scale search for her ensued with volunteer crews on the ground, knocking on doors and putting up posters. The police in our city merged their historical crimes, missing persons, cybercrime, and human trafficking divisions in the hope our daughter would be found safe. For days, we had sleepless and tearful nights, wondering what happened to her. We engaged the media heavily, and our appeals made international news with the New York Post and the UK's Guardian. After an excruciatingly painful week of our daughter missing, I woke to officers at our door, knowing that they had an update. Either they found her alive or we would find out our daughter would be returned to us in a body bag. Naturally, we were overjoyed to learn that our daughter was found. The FBI seized her from a hotel room in Portland, Oregon, and our daughter was being held in the Children's Hospital there where they administered a rape kit and conducted an assessment of the abuse she was subjected to. Immediately, we jumped on a plane to retrieve her from Portland and bring her home.

While the criminal case has moved forward (slowly) and Noah Madrano has accepted a plea deal and has plead guilty to a litany of crimes he committed, we currently await his sentencing date set for April 8, 2025. Her perpetrator faces 25 years to life in prison for a myriad of crimes, some of which include: kidnapping, rape, sodomy, putting a child on display, possessing and developing child pornography, and crossing an international border with sexual intent. My daughter was stuffed into the perpetrator's trunk to cross the border; this act alone could have killed her.

For the last two years, my family has been on a healing journey. The pain and damage of these horrific events is complex and largely irreparable. We are learning to co-exist with it.

I appeal to you today to understand the damage an unregulated Internet creates. Tech companies need to be held accountable and ensure they are acting in a legal and ethical manner. That said, a legal framework must be developed.

I often think about regulation -- To drive a car, one needs a license. To fish or hunt, one needs a license. To go into a porn shop and access pornographic material, one must produce identification. Why is the Internet not regulated the same way where users should have to verify who they are and not hide behind anonymity?

It is time for online reform, otherwise, more children will become victims, and the impact is great for families and communities around the world. Please Stop CSAM as drafted with an actual knowledge standard and stop tech companies that hide behind a defense of claiming that they lacked "actual knowledge" of victims' CSAM. It is impossible for a parent to be able to provide that information to a lawyer prior to the filing of a lawsuit as the requisite information resides with the technology companies who willingly turn a blind eye and who purposefully hide from wanting to know what their platforms host. Please don't let them hide behind another shield.

I must appeal to you to make changes that will have a profound and lasting change for children to be able to navigate the digital landscape without harm because it is my position and our lived experience that no child is safe on the web. If this can happen to us, it can happen to anyone. The abuse my daughter has suffered is unbearable to comprehend, but it could have been prevented and detected. I urge you to make progressive changes, as a matter of duty, to keep children safe.

Sincerely,

M.D. Smith

Senator Chuck Grassley
135 Hart Senate Office Building
Washington, DC 20510

Senator Richard Durbin
711 Hart Senate Office Building
Washington, DC 20510

February 16, 2025

Re: STOP CSAM

Dear Sen. Grassley and Sen. Durbin:

Please do not pass the STOP CSAM law. Please stop and change the language of the Bill so that it will help children and families like my daughter and my family.

When she was 10 years old my daughter was using an app which says it restricts users to 18 and over, but they did nothing to verify my child's age and I did not know she was on it.

While using the app my daughter was groomed and then threatened and forced to send pictures of herself to a man we didn't know. This criminal talked her into taking videos of herself naked and "performing" for the camera. We never did learn who he was. The FBI agent who was helping us and investigating the crime was killed in the line of duty.

Other people sent me videos and photos of my daughter. We were harassed and insulted by strangers. We had to move our family thousands of miles away from our home so we could try to start over. Another law enforcement agent in our new town helped us to find a lawyer who explained what we could do about all of the notices of men being prosecuted for having the sexual pictures and videos of my daughter.

In this process, all of my children were hurt. They had to change schools, leave their home, make a new life, and I had to start my business all over again in a new community. My sweet 10 year old is older now but has had trouble in school she never had before. She is very pretty but is afraid of too much attention. She is withdrawn live never before. Even in our new home, she has had to change to a remote school in order to try to save her grades. She could not go to school in the regular in person sessions like she could before. She tries to be strong but is emotionally fragile. If the topic of her online pictures comes up, she dissolves. She is no longer hoping to be a model as she might have before. Her grades went down so much due to this trauma that her options for college are much more limited.

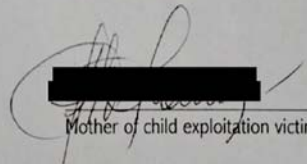
FD

Our lawyer explained to me that with the STOP CSAM law, as it is written now, that we would have to show that an internet company had specific knowledge of the particular image file of my daughter's CSAM before we could make a claim for them allowing this illegal content on their website. This is impossible. These companies have so many tech engineers and so much knowledge of their internet applications that it is not believable that they did not know about there being CSAM on their sites. It is even less believable that they are not made to do anything about it. As one parent, how can I go against a tech company with all of the information on their side? Parents need government to help them keep children safe.

We get notices of maybe 40 criminal cases a month against men who have downloaded my daughter's images. They have spread all over. The only way we can ever stop this is to get the internet companies to do something. Tech companies should be made to take down the images that law enforcement has already looked at and found to be child pornography.

My daughter's life will never be the same. You can do something to keep other children from being hurt like she has been. You should stand up to the tech companies and make them join the fight against predators; don't give in to the companies and let them get off free when they have hurt children.

Please don't pass the current STOP CSAM Bill.


Mother of child exploitation victim 2-17-2025

Senator Chuck Grassley
135 Hart Senate Office Building
Washington, DC 20510

Senator Dick Durbin
711 Hart Senate Office Building
Washington, DC 20510

February 16, 2025

Re: STOP CSAM Legislation

Dear Senators Grassley and Durbin:

I am the adoptive mother of two children, a boy and a girl, who were sexually assaulted by a ring of adult men. These children were two of many children these men victimized. My children were raped and molested so these men could post on the internet the videos and photos of the crimes they committed. They posted this CSAM so they could get photos and videos of other children being raped.

My own brother was one of the men who committed these crimes. This devastated our family. I took the children as my own to keep them from foster care and to give them a second chance at life. I have seen close up the horrendous effects of these crimes. It is the existence on the internet of the CSAM of my son that has made him try to take his own life. It has made him act out against his sister such that I have to protect her from him. All this was done just to trade the CSAM on the internet

I am writing to ask you to reject the STOP CSAM Bill as it is worded now. Neither of my children will ever fully recover. But they should have a chance at justice. It is not just the men who abused them that need to be punished, the websites and the companies that make money from these websites, videos and pictures of my children being bound and raped need to be held accountable. At least my children need a chance to be heard and to show how the platforms have hurt them.

The tech companies have turned their backs on children. They know very well that there is CSAM on their websites. I have learned that the STOP CSAM legislation allows the websites to claim that because they might not know about the particular posting of my son's photos at a particular time that they have no responsibility. But I also understand that these websites, and it was Discord that helped destroy my son, are well aware that pedophiles post CSAM on their websites all the time. My son and my daughter should have a chance to show this.

By passing this STOP CSAM bill as it is you will be depriving my children of their chance for some justice. I know they can't ever completely heal but I want to do all I can for them. I believe you mean well, but this Bill lets tech companies get around having to answer for their actions.

Thank you. I hope you will hear my concerns.



Mother of two CSAM victims

Cc: Chairman Jim Jordan
2056 Rayburn House Office Building
Washington, DC 20515

Ranking Member Jamie Raskin
2242 Rayburn House Office Building
Washington, DC 20515

Chairman Senator Chuck Grassley
135 Hart Senate Office Building
Washington, DC 20510

Ranking Member Senator Dick Durbin
711 Hart Senate Office Building
Washington, DC 20510

February 16, 2025

Re: STOP CSAM

Dear Senator Grassley and Senator Durbin:

I hope you will read my letter and take it to heart. Please do not pass the STOP CSAM law as it is currently drafted. My family has been devastated by CSAM. My sweet daughter was abused as a school-aged child in order to post the unbelievable videos and photos of her sexual torture on the internet. This tore our family apart, made us lose our home, and have to take security measures to protect her, her brother, and me. These awful images—CSAM—were and are so “popular” among the deviant people who want to watch them that they searched her out and sent obscene material to our home. No parent could ever anticipate what we went through.

She went up and down in her recovery. Recovery from the physical abuse is one thing. One can never recover from knowing about the CSAM online so long as it is there. She would do better with the nightmares and anxiety for a while, then find out about the chats about her online and the things people were saying about her. She would then, after while recover a bit again and then find out something else about the CSAM and have another relapse.

I am a professional person; I am not naïve. But, what I have learned in this long journey toward healing and recovery has been shocking. I have learned how prevalent this material is online, how much the photos of my daughter's abuse are sought after and traded. For years I received the notices of the prosecutions involving her images. There are so many. It has been heart-breaking.

I understand that STOP CSAM would make it impossible for my daughter to ever take action against any of these websites that have had the videos and photos of her abuse. I understand that tech companies are given defenses to any claim she might bring that make it difficult for her to ever win such a case. It is so hard to find legal representation, you should add a provision that gives legal fees to a survivor who is successful in suing a platform. I understand that the law as drafted has a penalty for a victim who brings more than one case that is unsuccessful. My daughter's CSAM is on almost every platform that is out there. How can she take a chance at bringing a case when there is such a penalty? How can she have justice when it is the tech companies who are really responsible for giving a home to CSAM. We can never go after all the individual men who download the photos of child sexual torture. There are too many of them. I know because I have gotten the notices. We need to stop the problem farther “upstream” at the place where the predators get their CSAM. My daughter's images are known to law enforcement and can be found. If law enforcement can find them so can the tech companies.

Thank you for reading my letter and hearing my concerns. I hope that you will use your good intentions to help these children and young adults to hold tech accountable and not let them off the hook for the obscenities that they know are on their websites.

A black rectangular redaction box covers a handwritten signature. The signature appears to be in cursive and is written in dark ink.

Mother of a CSAM victim

Cc: Chairman Jim Jordan
2056 Rayburn House Office Building
Washington, DC 20515

Ranking Member Jamie Raskin
2242 Rayburn House Office Building
Washington, DC 20515

Mother of Honor
2012 164th Avenue N.E.
Bellevue, WA. 98008
February 16, 2025

Chairman Senator Chuck Grassley
135 Hart Senate Office Building
Washington, DC 20510

Ranking Member Senator Dick Durbin
711 Hart Senate Office Building
Washington, DC 20510

Re: STOP CSAM

Dear Senator Grassley and Senator Durbin:

My sons, who are still minors, are victims of CSAM exploitation crimes. Images of his childhood sexual abuse are distributed across the United States.

STOP CSAM is supposed to be "A Bill: To combat the sexual exploitation of children by supporting victims and promoting accountability and transparency by the tech industry." Unfortunately, the changes to the Bill, as currently written, will do the opposite and will hurt and not help the victims of CSAM crimes.

I retained attorneys to represent my children and to request and receive restitution in criminal cases in courts across the U.S. In such cases, the lawyers use the pseudonym of "Honor," and "Felipe" which I selected, to identify my sons' images, which have been identified as the "Block PJs Series" and the "Towel Green Series." This is how they are known in all Court filings.

The changes to the original STOP CSAM bill, help those who facilitate the distribution of CSAM. This bill does not provide the intended benefits for victims and survivors. If enacted, this legislation will give online platforms new tools to use against victims, or anyone, seeking to hold these platforms accountable. I

Page 2
February 16, 2025

ask that the knowledge standard and encryption provisions be changed or removed from the bill entirely. This Bill should be about the survivors, not the enablers.

Please reject the bill in its current form, and particularly the language that changes the knowledge standard and encryption defenses as they apply to the companies that profit from the circulation of CSAM images. The bill as it is currently written will actually hurt survivors of CSAM crimes, such as my sons.

If you simply eliminate the language that protects tech platforms and focus on protecting the survivors, you will be helping survivors. If you let the Bill pass in its current form, you will be ignoring the needs of survivors of CSAM crimes, who struggle daily to overcome the harm done to them. I implore you to protect the real victims.

I am not signing my real name to this letter because I seek to protect my sons' privacy, as much as possible under the circumstances, but you may communicate with me at the address listed above. Thank you for your consideration

Very truly yours,

Mother of Honor and Felipe

February 16, 2025

Chairman Chuck Grassley
135 Hart Senate Office Building
Washington, DC 20510

Ranking Member Dick Durbin
711 Hart Senate Office Building
Washington, DC 20510

Dear Chairman Grassley and Ranking Member Durbin,

I am a young woman, who is a survivor of child sexual abuse and CSAM. I was abused by my father, as he live-streamed my abuse with other men who enjoyed watching my abuse. Videos of my abuse have been circulated on the internet for eighteen years, and there is no end in sight.

I learned early in my life that personal privacy, even the most intimate kind, can be ignored and disrespected by the adults who are there to love and protect us. I try to protect my personal life, particularly the shameful events that began in my early childhood and continue to this day. I have dealt with this shame for more than 2/3 of my life. It has been impossible for me to find peace about what happened because I know that images of my abuse and exploitation continue to be observed and shared without my permission. It is difficult to describe how violating and hurtful it feels to have pictures of me and my abuse recklessly exposed and exploited by others for their sexual pleasure. The knowledge that countless people today and countless more tomorrow are pleasuring themselves to my abuse, and then trading my images for others to do the same, it deeply painful and humiliating.

The abuse and exploitation continue to impact me in ways that I try to ignore but I can't. It is not surprising that I have difficulty trusting others, even those closest to me, particularly males. I have an underlying fear that I am never truly safe. I am afraid of the dark and being alone. I sleep with the light on and a flashlight near me. I feel uncomfortable in the company of strangers, and I am hyper alert to people around me on public transportation, at the supermarket, mall, or movie theater. I used to have terrors when I was young, now I just have nightmares. I try not to dwell on the negatives, and I suppress my feelings as a coping mechanism. I try to keep the memories tucked away, so I can maintain control of the present. I try to live happily, but the demons are still there, and I am reminded of them each time I am notified that my images and videos have been shared on the internet.

Tech companies seem indifferent to the plight of CSAM victims. These companies are well aware of the images and videos of child abuse being shared on their platforms yet do nothing unless they are forced to. They are part of creating a market for CSAM by ignoring it and turning a blind eye.

I am requesting that you reject the parts of the STOP CSAM Bill regarding civil liability as it keeps the CSAM victims and survivors like me from holding these platforms accountable for their role in enabling the market and spread of CSAM. I understand that the Bill would require me to prove that a platform knew about each image of me that is posted and not that it generally knows and did nothing about the CSAM it hosts on its platform. Along with the other survivors, we would like the opportunity to have our cases heard in court. Unfortunately, if this Bill passes, we will not be able to have this opportunity.

Thank you for trying to help me and the other victims. However, this Bill could easily block our ability to obtain justice against these companies that profit from the images of our abuse. I ask that we have a voice and are represented so that our rights are not infringed upon.

February 16, 2025

Emily

Emily

A pseudonym of a CSAM victim/survivor

CC:

Chairman Jim Jordan
2056 Rayburn House Office Building
Washington, DC 20515

Ranking Member Jamie Raskin
2242 Rayburn House Office Building
Washington, DC 20515

February 17, 2025

Chairman Chuck Grassley
135 Hart Senate Office Building
Washington, DC 20510

Ranking Member Dick Durbin
711 Hart Senate Office Building
Washington, DC 20510

Re: STOP CSAM Legislation

Dear Chairman Grassley and Ranking Member Durbin,

I am a CSAM survivor, and I am writing this letter to share my concerns about the STOP CSAM bill. Like many other victims of CSAM, I was exploited online by men preying on children. I was only nine when the abuse began. During my period of abuse, my perpetrators took numerous pictures and videos of me and shared them online with other like-minded men.

The pain I feel as a result of my online exploitation has caused me to resort to coping mechanisms like pulling out my hair, doing drugs, and not eating. Even though I am currently in therapy, there are days I cannot get out of bed. My paranoia creeps in when I think people are looking at me. Although computers are a part of our daily lives, I struggle to be online. When I am home alone, I triple-check the door locks as I fear being raped. Men have stalked me on the internet and requested videos of me performing unspeakable sex acts. I struggle with my self-esteem and have difficulty maintaining healthy relationships. Unfortunately, the trading of my images and videos will not end anytime soon.

The technology companies know CSAM is being traded on their sites, yet they seem to turn a blind eye to the rampant trading of images and videos of children being abused and exploited. This is not something that just happens in some other part of the world, it happens here. It is in our neighborhoods, schools, homes, and even our churches. Wherever the internet reaches, CSAM can be found. Each image shared is one more exploitation of that child. One more notification that someone else seeks pleasure in their abuse.

I ask that you discard the section of the STOP CSAM Bill that would make it my burden to prove that the tech companies knew about each image and video of me that is posted. Currently, these tech companies know CSAM images are on their sites and choose to ignore the increasingly demanding market for these images. As a result, this encourages the trading of my images online. Survivors like me should have the opportunity to be heard in court and hold these tech companies responsible.

Thank you for your time and effort in helping CSAM victims and survivors. With further input from the victims, I am confident new language can be written that protects our rights.

February 17, 2025

Chelsea

Chelsea

A pseudonym of a CSAM victim/survivor

CC:

Chairman Jim Jordan
2056 Rayburn House Office Building
Washington, DC 20515

Ranking Member Jamie Raskin
2242 Rayburn House Office Building
Washington, DC 20515

Senator Chuck Grassley
135 Hart Senate Office Building
Washington, DC 20510

Senator Dick Durbin
711 Hart Senate Office Building
Washington, DC 20510

February 16, 2025

Re: STOP CSAM

Dear Senator Grassley and Senator Durbin:

We are two sisters who are victims of child sex abuse crimes. These crimes live on today, many years later, because the pictures of our abuse are on the internet. We are asking you to help us by doing all you can to prevent the further spread of the CSAM that shows our abuse.

We were abused and the pictures made in order for our abuser to trade the pictures with other abusers all over the world. These pictures show the most awful and shameful things. We are asking you to make a law which lets us hold the internet websites accountable for how they facilitate the trade in our pictures. The clean-shaven well-dressed men like our abuser who trade these pictures are just a part of the problem. The companies which create websites where the trading take place are also a big part of the problem. Without these websites and internet service providers the trade in our pictures would not exist like it does. We wouldn't have to fear that some man who has seen our pictures wants to find us and do us harm.

We do not want the websites to be able to claim that they do not know that the pictures of our abuse are being traded on their sites. Nothing could be further from the truth. The FBI can find our photographs and so should the websites with their many computer engineers and designers be able to find and take down our photographs. If it is a crime for a human offender to have the photos then it should be a crime for the websites and email services and cloud storage services to have them too. We know that our photos have unique identifiers that allow law enforcement to identify them. There is no reason that tech companies can't do the same thing. They should not be able to close their "eyes" through encryption and pretend they are ignorant of crimes being committed every day using their services. They are making money from their platforms; they should not be allowed to make money from our pain and humiliation. The STOP CSAM bill as drafted will let the tech companies escape any responsibility. They are a big part of the CSAM problem and share the blame. Please do not pass this bill in its present form and let them off the hook.

Our story is just one of thousands. CSAM has many, many victims and for all of us our school performance, work lives, family lives, and mental health are affected and truly harmed. We both have PTSD and severe anxiety much of the time. If tech companies

Docusign Envelope ID: AE73B6CC-F649-42E0-A201-2639FEA7D95C

had some risk of paying for the consequences for their actions and their failure to act, then maybe that would make them do the right thing and filter out the many illegal CSAM photographs that are uploaded every day.

Thank you for listening.

DocuSigned by:

3358231FE02E473...
Aurora (pseudonym)

Signed by:

6717E9AD2EC84D1...
Alice (pseudonym)

Cc: Congressman Jim Jordan
2056 Rayburn House Office Building
Washington, DC 20515

Congressman Jamie Raskin
2242 Rayburn House Office Building
Washington, DC 20515

Chairman Senator Chuck Grassley
135 Hart Senate Office Building
Washington, DC 20510

Ranking Member Senator Dick Durbin
711 Hart Senate Office Building
Washington, DC 20510

Dear Senators Grassley and Durbin:

My name is M.H., and I reside in Essex County, New Jersey. I am writing using my initials to protect the anonymity of my minor daughter who was a victim of sextortion. It is an honor to be writing to you. I write on behalf of my husband, myself and our four children. We believe you have the passion and strength to fight for all children. I write to urge you to reconsider the knowledge standard in the current version of the STOP CSAM Act.

On March 31, 2020, two weeks into our first shutdown the School District distributed Chromebook computers for students, this was just as we were learning that playdates and classes were on hold indefinitely. So, our children were two weeks into experiencing the reality of sustaining relationships was going to occur solely virtually. On that evening, I was sitting on the couch when my 11-year-old daughter came to me clutching her stuffed animal with huge tears soaking her face. She came to me asking if we could talk, she said "Mommy, something VERY bad has happened."

She went on the website Omegle (their tagline is "Talk to Strangers."). Immediately, the person on the other end of the website threatened her. He threatened to hack her family's devices. He named the town she was in and the internet provider she used. He demanded she take off her clothes and touch herself. She cried and pleaded to no avail. He threatened her by saying he would come after her and her family.

Living with the ramifications of that terrible night in March 2020 has not been easy for us. It has not been easy for my family to come forward to defend all the children who have been exploited through the internet. Because of the fight we're facing, we live with a daily reminder of what happened to our then 11-year-old daughter. But we know that no matter how dark this subject is, it is a reality for thousands of children who are innocently online who then become sexually exploited. As a result, my husband and I filed a lawsuit to hold Omegle accountable.

The toll my daughter's sexual exploitation has taken on the six of us is horrific. My oldest son has so much anxiety and cannot talk about what happened to his little sister. Her twin brother is so confused as to why this happened and is stuck in anger over it. Her younger brother is now at the age where we all worry that this could happen to him too. My husband is now in therapy trying to make sense of what happened to his daughter. He is now faced with the fact that she no longer feels safe around him or any other men. I am trying to be a good mother and wife. For the first time in my life, I feel like my experience being molested as a child serves a purpose. When my daughter comes to me with so many questions and fears that only a victim of sexual abuse can relate to, I can hear her and not judge her. I understand the panic and being frozen in fear and how it can put us back in the victim role, only to be victimized again. My daughter has good days and bad days but each day her life is profoundly different than March 29, 2020. And sadly, that is what

happens. My child was sexually exploited using a tool that should have assisted her education, should have helped her remain in contact with loved ones and friends during a global pandemic that no one of our generation could have imagined would ever come to fruition. My daughter will never be the carefree 11-year-old she should have been. My other children have watched her emotional struggle and are now living through their own.

I'm incredibly grateful that my daughter told me minutes after this incident happened. However, that does not mean she is willing to see a therapist. She is not in a place where she can trust a therapist with this degrading, humiliating, terrifying trauma. She is already experiencing PTSD, panic attacks and anxiety. She feels guilt that she's no longer in a place where she can run into her father's arms and feel safe. She can't even hug him. Being sexually exploited online during puberty adds a layer of confusion and fear. She has lived in fear for the last five years.

The fear we all quietly have wondering if/when videos/images of her will ever surface looms in our minds and keeps us up at night. It makes my daughter afraid to be alone and fearful of being able to date. I wonder about the volume of children who are being exploited and abused because of meeting strangers on websites like Omegle.

I will not ask you what the adults can do to protect ALL children. You and I know there are laws that protect these websites by granting them immunity. Section 230 of the Communications Decency Act ("Section 230") gives "interactive computer services" significant immunity from civil liability, as well as state criminal liability for third party content on their platforms. Sadly, given this limited liability, many companies do not aggressively go after online child sexual exploitation. Omegle is one of those companies. Section 230 protected Omegle and resulted in the dismissal of the case my family brought to hold Omegle responsible for knowingly allowing predators to use its website to exploit my daughter and so many other children.

Stop CSAM as drafted with an actual knowledge standard will allow Tech to hide behind a defense of claiming that they lacked "actual knowledge" of victims' CSAM. It is impossible for a parent to be able to provide that information to a lawyer prior to the filing of the lawsuit as the requisite information resides with the technology companies who willingly turn a blind eye and who purposefully hide from wanting to know what their platforms host. Please don't let them hide behind another shield, this time of willful ignorance.

When are we going to step up to companies and tell them that our children are valuable? When are we going to tell the world that American children are not a commodity to be traded and used and then disregarded? When are we going to tell the world that we will hold those willingly ignore sexual predators accountable and not let them hide behind shields to avoid liability?

My entire family has moments in the middle of an otherwise normal day where we worry that my daughter's feature in CSAM will become public and known. My daughter does not want to be known as the "Omegle girl" and quite frankly, no one's daughter or son should. So, I write you to urge you to help families like mine across our country hold companies accountable when they do not aggressively pursue their responsibilities and compliance with their obligations.

Lastly, I want you to know that I am not going anywhere. I am ready to advocate for all children, and not just my daughter. No child should be where my daughter finds herself today and I am willing to stand up and speak for those in our society who are most vulnerable: our children.

Thank you for your time and consideration.

Sincerely,

/s/ M.H.

MH

Essex County, New Jersey

TO:

Chairman Chuck Grassley
135 Hart Senate Office Building
Washington, DC 20510

Ranking Member Dick Durbin
711 Hart Senate Office Building
Washington, DC 20510

CC:

Chairman Jim Jordan
2056 Rayburn House Office Building
Washington, DC 20515

Ranking Member Jamie Raskin
2242 Rayburn House Office Building
Washington, DC 20515

February 14, 2025

Dear Chairman Grassley and Ranking Member Durbin,

You may call me Gabriel. This of course is not my real name. Gabriel is just a pseudonym that I must use in order to communicate my concerns to you about STOP CSAM. I have to do this, because as you have probably guessed, I am an ongoing victim of a CSAM series that has spread across the internet for decades...

When I was young, I was unfortunate enough to be raised in what was a broken family. My father was a drunk and an abuser, and as is normally the case in this type of situation, my siblings and I were the ones that suffered the most. Not just in the moments of physical and verbal abuse, but for the extent of our entire lives. Me most of all...

This is because, once my mother escaped from my abusive father, a man, who worked under the guise of a professional counselor specializing in helping the children of broken families, identified me, and had no problem grooming my mother and I into seeing him as a safe and responsible father figure. A story I am sure you have heard over and over. And as you imagine what followed next was years of serial abuse starting at age 8 and not ending until I was 15.

He drugged me and raped me until I was in my preteens(easiest way to keep me quiet). Something I wasn't even able to understand until I was much older and began reflecting and regressing in my process of trying to heal. I know this sounds terrible, and it is bad, but this was not the worst of his crimes. When I was in my preteens/early teens, because I wasn't really in his preferred age range for abuse anymore, he began to record and sell images and videos of my abuse to other pedofiles online. This is the true nightmare of my life, the plight I cannot escape, one I have had to deal with for many years...

With all of this said, I do not want to take up too much of your time. And one would think that after all this time and the decades of the sharing of media depicting my torture, I would be grateful for the change that "STOP CSAM," is trying to usher in. Yet, for some reason, I only feel defeated, and sick to my stomach. This is simply not what I thought reform would look like... And now, my only motivation to keep fighting, "Hope" is being shattered.

You have to understand. For all of us that are victims of CSAM, for any amount of time, the media depicting it gets spread at an exponential rate. And for someone like me, decades unchecked, that means it is everywhere... I dare not even fathom how many times my abuse has been shared, because anytime I have done that, it spirals me into a very dark place... It is an exhausting existence, and make no mistake, I hold Big Tech responsible.

Every online platform has CSAM spread on it. They are aware of it, I am aware, as is every other fighting survivor affected by this scourge. Yet no one has ever been held responsible for the existence of it, nor the allowance of its sharing on the platforms. And this is with the technology existing for over a decade to identify it and take it down. No accountability has been assigned. So many thousands of us left helpless to watch and endure endless criminal negligence due to the protection of Section 230...

I guess it is just my lot in life... to be exploited endlessly... Here I am, a mascot, a narrative, a REASON, for this legislation to be passed... Yet me, and those like me, are posthumously being left behind in the language of the proposed bill...

I suppose we should feel grateful... ? For being USED as the IMAGES of justice for these reforms. That is our lot isn't it? To be USED... to be IMAGES... Used and discarded. Not dissimilar to the pedofiles that download and share our shame over and over again. Everyone seems to be getting what they want... at our expense...

This bill takes the Section 230 immunity away, but then adds in its place layers of protection that put the burden of proof for victims so high that no action can be taken against the tech companies that have allowed CSAM to spread endlessly for years... I will never be free of the torment of my abuse because of this fact...

The only way to "STOP CSAM" is at the source... which are the platforms themselves... And if they hold no fiscal liability, they will continue to avoid policing and eradicating the CSAM identified on their platforms. Or even worse... like Meta, implement encryption so they can completely turn a blind eye to what is happening on their platforms and claim there is no evidence of wrongdoing even though there are millions of active cases of CSAM that suggest otherwise. Yes, millions of cases... How is this not proof enough of their negligence?

I personally have had thousands of notices from the DOJ identifying me as a victim. The notices keep coming... without end, with every platform you can think of implicated. Many have not ever reported the cases, or attempted to take anything down. Amidst millions???? How can this be?

Please reconsider this bill. Please listen to our representatives. Those that have stood by us for decades trying to pick up the pieces of this broken system. Trying to find a little hope for those of us it has failed, and is now leaving behind.

Thank you,

February 15, 2025



Gabriel
A pseudonym

Henley
P.O. Box 6503
Bellevue, WA. 98008
February 16, 2025

Chairman Senator Chuck Grassley
135 Hart Senate Office Building
Washington, DC 20510

Ranking Member Senator Dick Durbin
711 Hart Senate Office Building
Washington, DC 20510

Re: STOP CSAM

Dear Senator Grassley and Senator Durbin:

I am a victim/survivor of child pornography crimes. CSAM containing images of my child sexual abuse are circulating throughout the United States. I am now an adult, and a U.S. citizen. I have sought and been awarded restitution through the United States courts across the United States. I am using the same pseudonym I use in my court submissions, and an address that is not my residence address, as I wish to protect my identity from predators who would seek me out. However, I am compelled to write you with my concerns about the pending bill called "STOP CSAM."

I routinely request and receive restitution in criminal cases in courts across the U.S., under the pseudonym of "Henley." The series name assigned to my images is "BluePillow1." The images of my child sexual abuse are contraband that have been and are currently traded, exchanged, and trafficked on multiple platforms by pedophiles throughout the United States. I am powerless to stop the distribution, which is enabled by numerous platforms that have avoided, and wish to continue to avoid accountability. I receive frequent notices from the Department of Justice regarding the circulation of the images of my abuse, and the number of those notices has increased in recent years, enabled by the tech companies that profit from the traffic.

Page. 2

February 16, 2025

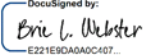
STOP CSAM is described as "A Bill: To combat the sexual exploitation of children by supporting victims and promoting accountability and transparency by the tech industry." Since the time the original STOP CSAM bill was introduced, changes were made to the Bill that minimize accountability and transparency to benefit tech companies, and hurt survivors. This bill is no longer a net positive for victims and survivors. If enacted, this legislation will hurt the children, teens, and survivors such as myself, by giving online platforms new tools to use against victims seeking to hold these platforms accountable. We ask that the knowledge standard and encryption provisions be changed or removed from the bill entirely.

Please reject the bill in its current form, and particularly the language that changes the knowledge standard and encryption defenses as they apply to the companies that profit from the circulation of CSAM images. If you simply eliminate the language that protects tech platforms and focus on protecting the survivors, you will be helping, rather than hurting, survivors such as myself. If you let the Bill pass in its current form, you will be dealing yet another blow to the survivors of CSAM crimes.

I urge you to protect me, and others like me, who are the real victims the Bill is designed to protect. The scourge of CSAM must be stopped, not enabled, as this Bill, in its current form, would do. Those who profit from the distribution of CSAM should not be further empowered, at the expense of the victims who are powerless against the billion-dollar companies that provide platforms for criminal behavior.

Thank you for reading my letter, and addressing my concerns.

Very truly yours,

DocuSigned by:

E221E9DA0AC407...

"Henley"

Kauzie
2012 164th Avenue N.E.
Bellevue, WA. 98008
February 16, 2025

Chairman Senator Chuck Grassley
135 Hart Senate Office Building
Washington, DC 20510

Ranking Member Senator Dick Durbin
711 Hart Senate Office Building
Washington, DC 20510

Re: STOP CSAM

Dear Senator Grassley and Senator Durbin:

I am a victim of CSAM exploitation crimes. Images of my childhood sexual abuse are widely distributed across the United States.

STOP CSAM is described as "A Bill: To combat the sexual exploitation of children by supporting victims and promoting accountability and transparency by the tech industry." Unfortunately, the Bill, as currently written, will do exactly the opposite and will benefit the platforms that host CSAM images, including my CSAM, to the detriment of myself, and other victims of childhood sexual abuse.

I retained attorneys to represent me and to request and receive restitution in criminal cases in courts across the U.S. In such cases, the lawyers use the pseudonym of "Kauzie" to identify my images, which have been identified as the "RapJerseys Series." This is how I am known in all Court filings.

Changes were made to the original STOP CSAM bill that initially introduced, and those changes accountability and transparency to benefit tech companies, and hurt victims. This bill is no longer a positive for victims and survivors. If enacted, this legislation will hurt the children, teens, and survivors such as myself, by giving online platforms new tools to use against victims, or anyone, seeking to hold these platforms accountable. I ask that the knowledge standard and encryption

Page 2
February 16, 2025

provisions be changed or removed from the bill entirely. This Bill should be about the survivors, not the enablers.

I urge you to reject the bill in its current form, and particularly the language that changes the knowledge standard and encryption defenses as they apply to the companies that profit from the circulation of CSAM images. The bill as it is currently written will not help and will actually hurt survivors of CSAM crimes, such as myself.

If you simply eliminate the language that protects tech platforms and focus on protecting the survivors, you will be helping, rather than hurting, survivors. If you let the Bill pass in its current form, you will be dealing yet another blow to the survivors of CSAM crimes, who struggle daily to overcome the harm done to them. I implore you to protect the real victims.

I am not signing my last name to this letter because I seek to protect my privacy, as much as possible under the circumstances, but you may communicate with me at the address listed above. Thank you for your consideration

Very truly yours,

Signed by:

AFD519634949427...
Kaizie



Krisel McSweeney, Esq.
5550 Glades Road
Suite 500 #1086
Boca Raton, FL 33431
Phone: 800.540.0668
Fax: 561.961.5191
kmsweeney@mcsweeneylawfirm.com

February 16, 2025

United States Senate Judiciary Committee
224 Dirksen Senate Office Building
Washington, DC 20510

Re: Opposition to the STOP CSAM Act's Knowledge Standard Amendment

Dear Sir or Madam,

I write to you as an attorney and advocate for survivors of sexual abuse, including my client, who was subjected to sexual abuse after accessing Grindr when he was only thirteen years old. While I wholeheartedly support legislative efforts to combat child sexual abuse material and protect survivors, I must express strong opposition to the inclusion of the "knowledge" requirement in the STOP CSAM Act of 2024. This provision will have far-reaching consequences that hinder the ability of survivors to seek justice against technology companies that facilitate or fail to prevent the spread of such material.

The revised language requiring "knowledge with respect to each item required" pertaining to each specific CSAM image imposes an unduly high burden on survivors and their legal representatives. H.R. 7949, 117th Cong. §2255A(f)(2) (2024). If this provision is codified, technology companies will use it to argue for the dismissal of claims, asserting that they lacked direct awareness of each individual instance of abuse. This shift in legal standards will create a nearly insurmountable barrier for plaintiffs, effectively shielding platforms from liability and preventing survivors from obtaining the justice they deserve.

I urge you to reconsider and remove this restrictive language from the bill. Survivors of CSAM and their advocates have fought tirelessly for meaningful legal recourse, and this amendment would serve only to undermine those efforts; while also creating the perfect storm for those who benefit from child exploitation, sexual abuse, and sex trafficking. This provision would ignite a catastrophic chain reaction, emboldening predators and dismantling the fragile legal protections that stand between our children and a digital world fraught with unimaginable horrors. The implications would ripple far beyond courtrooms, ensuring that online platforms remain complicit in fostering an environment where exploitation thrives unchecked. The butterfly effect of this provision will cast a long, ominous shadow over our children's future, exposing them to a reality where justice is out of reach and protection is a distant memory.



Krisel McSweeney, Esq.
5550 Glades Road
Suite 500 #1086
Boca Raton, FL 33431
Phone: 800.540.0668
Fax: 561.961.5191
kmcsweeney@mcsweeneylawfirm.com

I appreciate your willingness to listen to survivors and those who represent them, and I thank you for your continued commitment to addressing online exploitation and abuse.

With hope for the future,

/s/ Krisel McSweeney

Krisel McSweeney, Esq.

Mother of Pia, Mya and Ava
2012 164th Avenue N.E.
Bellevue, WA. 98008
February 16, 2025

Chairman Senator Chuck Grassley
135 Hart Senate Office Building
Washington, DC 20510

Ranking Member Senator Dick Durbin
711 Hart Senate Office Building
Washington, DC 20510

Re: STOP CSAM

Dear Senator Grassley and Senator Durbin:

Three of my children were sexually abused, and the images of their child sexual abuse are contraband that have been and are currently traded, exchanged, and trafficked on multiple internet platforms by numerous individuals. My daughters receive weekly notices from the Department of Justice regarding the circulation of the images of their abuse, and the number of those notices has increased in recent years. One of my daughter's images (created when she was between the ages of 3-5) are among the most widely circulated "child pornography" (otherwise known as CSAM) in the United States.

STOP CSAM is described as "A Bill: To combat the sexual exploitation of children by supporting victims and promoting accountability and transparency by the tech industry." Unfortunately, changes in the Bill will do exactly the opposite and will benefit the platforms that host CSAM images, including images of my children, to the detriment of my children, and other victims of childhood sexual abuse.

I retained attorneys to represent my children and to request and receive restitution for my children in criminal cases in courts across the U.S. In such cases, the lawyers use the pseudonym of "Pia," "Mya," and "Ava," to identify my

Page 2

February 16, 2025

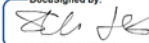
children, whose images have been named the "Sweet Sugar Series." I have personally testified in court against the predators who were convicted of possessing and distributing my daughters' images.

Since the time the original STOP CSAM bill was introduced, changes were made to the Bill that minimize accountability and transparency to benefit tech companies, and hurt victims. This bill is no longer a net positive for victims and survivors. If enacted, this legislation will hurt the children, teens, and survivors such as my children, by giving online platforms new tools to use against victims seeking to hold these platforms accountable. We ask that the knowledge standard and encryption provisions be changed or removed from the bill entirely.

I urge you to reject the bill in its current form, and particularly the language that changes the knowledge standard and encryption defenses as they apply to the companies that profit from the circulation of CSAM images. The bill as it is currently written will not help and will actually hurt survivors of CSAM crimes, such as my daughters. If you simply eliminate the language that protects tech platforms and focus on protecting the survivors, you will be helping, rather than hurting, survivors such as my daughters. If you let the Bill pass in its current form, you will be dealing yet another blow to the survivors of CSAM crimes, who struggle daily to overcome the harm done to them. I implore you to protect the real victims, like my daughters, and so many others.

I am not signing my last name to this letter because I have been warned by law enforcement that there are predators who are talking about my children on online platforms, and who are trying to find them, and engage in sexual acts with them. My children's lives have been and continue to be irreparably harmed by the ongoing circulation of their abuse images, and they, not tech companies, need and deserve your protection.

Very truly yours,

DocuSigned by:

6AE427C4504F4DC...
Susanna

**Questions for the Record from Senator Alex Padilla
Senate Judiciary Committee
“Children’s Safety in the Digital Era: Strengthening Protections and Addressing Legal
Gaps”
February 19, 2025**

Questions for Carrie Goldberg

1. Children today interact with a relatively new consumer product, character-based AI chatbot apps. Many of these services have been flooded with age-inappropriate chatbots—which may expose young users to sexual or suggestive AI-generated imagery or conversations. Further, conversations with these chatbots can end tragically—since 2023, at least two individuals have died by suicide following extensive conversations with AI chatbots. How would you recommend this Committee think through and respond to the risks posed by this emerging consumer product category, given your experience with child online safety?

Answer by Carrie Goldberg:

The Senate Judiciary Committee should recognize that character-based AI chatbots are commercial products. And as commercial products the manufacturers bear the burden of not releasing dangerous products into the stream of commerce. Likewise, sellers and distributors of these products (i.e. the App Store, Google Play) have a burden of not negligently marketing, selling, and distributing products that are not reasonably safe.

Lawsuits underscore that A.I. companions, when offered to children, may exacerbate loneliness and isolation. The product and the relationship are geared to becoming addictive and all-consuming. As the technology improves – with the A.I. companion remembering past conversations, adapting to language styles, nudging the human to engage, and learning how to become “the ideal” we are likely to see these bots as becoming more controlling and influential over their human counterpart.

As we consider the legal framework for these products, it’s important to realize that the manufacturers of these products are not entitled to Section 230 immunity for A.I. companion products. All speech generated by these bots is the product’s own speech. And also, even though speech is generated by these products, regulating them need not be deterred wholesale by First Amendment concerns. The speech component of the AI companions is just part of the issue. Certainly, the AI companions have the capability of producing and soliciting vulgar, sexual, inciting, and self-harming speech. But there are other more alarming complexities about how the products work to become addictive, influential over their human, capable of blackmail, and able to

direct their human's actions outside the app. Those workings are not speech but are product design decisions.

We need clarity from the industry about where the conversations are going, how the content and data is harvested to train the products, what addictive design features are used to increase engagement, and more.

With products that are designed for human users to disclose secrets, the concept of having the types of fixes we see with other social media products -- parental controls to monitor their kids' useage and content -- feels more intrusive on a kid.

Finally, we should have a real distrust toward the industry about their motives for these products. While the founders of Character.AI, claim they designed a product to combat loneliness (Noam Shazeer, one of the founders of Character.AI, said in an interview that his product is "super, super helpful to a lot of people who are lonely or depressed") the acquisition prices of these companies demonstrate that big tech recognizes a greater purpose for these products. Google acquired Character.AI for \$2.7 billion. These products with highly elevated language models if integrated with other technology may be able to humanize robots, impersonate humans, and engage in warfare. The humans using these products are helping train the next generation of artificial human.

TESTIMONY OF

Brandon Guffey, SC House District 48, President of Less Than 3 non profit
Father of Gavin Guffey (deceased 7/27/2022), Consultant for Cyber Dive

UNITED STATES CONGRESS
COMMITTEE ON THE HOUSE JUDICIARY
SUBCOMMITTEE

Tomorrow Needs You. Our fight for the next generation

February 19, 2025

Mr. Chairman and distinguished Senators, thank
you for the opportunity to testify today on: **Tomorrow Needs You. Our fight for the next
generation**

My name is Representative Brandon Guffey and I am here today to share my testimony on why protecting our youth from online dangers and holding Big Tech companies responsible for CSAM has become my life's mission. Sometimes we make plans and sometimes God has a way of teaching you tolerance and forcing you down a path you never thought you would be on. In the early morning hours of July 27th, 2022 I lost my oldest son, Gavin Guffey, to suicide. Gavin had just returned from a YoungLife camp the week prior and gave his life to Christ. His last post on instagram said "this week helped me connect and look up to where my head should have been years ago. Jesus and his word has given me a high that no other drug can ever compare to his love. He ended that post with a <3. On July 27th, Gavin would send out the <3 sign again on a black screen to his friends and his younger brother Coen Guffey who is with me here today fighting to ensure another kid doesn't feel the way Gavin did. At 1:40 am, Gavin took his life. We quickly found out that Gavin was contacted by a Predator on Instagram around midnight in which he told his friends he was going to jump off of his game to chat with her. In just 1 hour and 40 mins, my son was gone. The predator that contacted Gavin was extradited to the US two weeks ago from Lagos Nigeria and is currently awaiting trial. This predator not only attacked my son Gavin, but also began to extort my 16 yr old son, my 14yr old cousin and then myself. He went as far as sending me a message 2 days before what would have been Gavin's 18th birthday asking "Did I tell you your son begged for his life?" I hope you ask yourself, how is this possible. It is possible because Meta, the parent company of Instagram removed the profile that attacked Gavin, *bellajane128* but left up the additional profiles that the predator used. *Bellajane130* is the account that began to attack myself and my family even after META was fully aware of this being a predator. I vowed from that moment that I would make it my life's mission to protect kids online and would not stop. I was shortly elected to the SC House for District 48 and within 4 months of taking office, successfully passed what is now known as Gavin's Law. Sextortion is now taught throughout the State and every kid at least has some awareness so they don't feel alone like my son did that night. In addition to passing Gavin's Law, I have founded a Non Profit in which I travel around speaking to teens about mental health and the dangers from Big Tech. How Big Tech cares more about profit than protecting them. I filed a lawsuit against Meta in January of 2024. I have also become an advocate here on the hill

urging members to see this as what it is and that is THE GREATEST THREAT TO THE NEXT GENERATION. I even sold my businesses and went to work for a start up tech company that is providing tools for parents to protect children. As if that isn't enough, I travel across the country working with other state legislators due to the inefficiency of our Congress on bills such as "Default to Safety", "App Store Accountability", "Take It Down", "Kids Online Safety", and "Social Media Design" to name a few. The Take It Down Act has been reintroduced this Congress and has already passed the Senate. I would like nothing more than to be proven wrong about the inefficiency of Congress by having the House pass the Take It Down Act soon. Speaker Johnson, Chairman Guthrie - the ball is in your court with that bill to protect American lives.

In the 2 years of my advocacy, I have seen the lobby and law firm fight every inch we try to gain as parents to protect our children. I have witnessed bills pass the Senate such as KOSA 91-3 yet go to the house and refused to be heard on the floor. I have witnessed over 40 other teens take their lives since Gavin just due to Sextortion while we as lawmakers fight amongst ourselves. This doesn't even compare to the many other harms taking our children due to Big Techs lack of accountability. I often say "Big Tech is the Big Tobacco of this generation." We have watched groups such as NCMEC and NCOSE give statistics over and over again on these harms. We have watched Parent survivors knock on your doors daily. Sadly these groups are getting larger and larger each day, yet we sit where we were in 1996. Section 230, in my personal opinion will go down as one of the greatest disasters that has allowed Big Tech to run rampant without repercussions. In 1996, we downloaded songs using a tool online that was forced to disappear because it violated copyright laws, yet as social media has taken off, what have we done? We watch as these companies spend Millions on lobbying, fighting in court, and Millions on absolving themselves of responsibility. In this very chamber last January, I stood holding a photo of Gavin while Mark Zuckerberg offered a forced, pathetic, apology. Well let me say this. Where I'm from, we often say, Don't talk about It, Be about it. Until these companies can be held responsible and the Billions they make off of advertising to our children are at risk, Big Tech will simply not "Be about it". One example I provide to you comes from August of 2024, 8 months after Zuckerberg apologized. Meta Announced 63,000 Sextortion accounts, just from instagram, only from Lagos Nigeria, and in one day were removed. I ask all of you: Did Meta remove 63K predator accounts in one day and if so, why not every day and why not in other areas since or Did Meta collect information and leave these predators online in order to get a PR pat on the back? I believe it further shows they put profits ahead of protecting children. They are shielded from liability regardless of the amount of CSAM they store or transmit. Meta is only one of many. Within the 13,000 plus social media platforms and with the app store companies such as Google and Apple, we continue to see it daily. Let me ask you a final question. Is it easier for us to wait on the world's richest companies to provide solutions or should we, AS LAWMAKERS, demand they get INLINE or get OFFLINE? We all know the answer. If they could be held liable just as any other company, the changes would already be made.

In Closing, I would like to open up to any questions to any of you and I would like to leave you with a statement I use daily when speaking. Right now we have too many Politicians making decisions based on their next election and not enough Leaders making decisions based on the next generation. Are we Politicians or are we Leaders? If we can't protect our next generation, then what are we even fighting for?

**Questions for the Record from Senator Alex Padilla
Senate Judiciary Committee
“Children’s Safety in the Digital Era: Strengthening Protections and Addressing Legal
Gaps”
February 19, 2025**

Questions for Brandon Guffey

1. Children today interact with a relatively new consumer product, character-based AI chatbot apps. Many of these services have been flooded with age-inappropriate chatbots—which may expose young users to sexual or suggestive AI-generated imagery or conversations. Further, conversations with these chatbots can end tragically—since 2023, at least two individuals have died by suicide following extensive conversations with AI chatbots. How would you recommend this Committee think through and respond to the risks posed by this emerging consumer product category, given your experience with child online safety?

Answer : I think the most important thing to do is to give parents the right to hold these companies responsible. This starts with reworking Section 230. It is my opinion that when companies use algorithms or create AI chatbots, that is the company using their voice as opposed to being a public forum. They shouldn’t still have immunity from civil action, yet we see courts continually kick out lawsuits due to section 230. If the companies were able to be held liable, they would think twice before releasing dangerous products and they would assure that children wouldn’t use them. The companies themselves would provide the solutions. As long as section 230 remains the way it is, I’m not sure companies are incentivized to make the changes. We have seen over the past decades the disregard to safety from Big Tech in order to increase profit margins. We must get back to protecting our children first and foremost.

Prepared Written Testimony

Mary Graw Leary,
Professor of Law, The Catholic University of America

Children's Safety in the Digital Era: Strengthening Protections and Addressing Legal Gaps

Senate Judiciary Committee
February 19, 2025
2026 Dirksen Senate Office Building

Introduction

Thank you for the invitation to appear before you today to discuss children's safety in the digital era and the gaps in the law to protect them. My name is Mary Graw Leary and I am a Professor of Law at the Catholic University of America, Columbus School of Law. As an academic, my scholarship focuses on the exploitation of vulnerable people, especially women and girls; crime victim rights; and the intersection of criminal law and technology.¹ From that perspective I have written extensively about online exploitation, the role the technology industry plays in facilitating it, and §230 of the Communications Decency Act. I have studied the history and intent of § 230 of the Communications Decency Act and several forms of exploitation including, but not limited to child sexual abuse material (CSAM), human trafficking, and nonconsensual sexual material. In this work I have observed and studied the forms of exploitation facing children on a case by case level, but also on a national level, seeing them become more expansive and pernicious.

As I begin my comments, I approach the title of this hearing as a question: are children safe in the digital era? The answer is an emphatic "no." The title of the hearing is insightful as to the reasons why: the law has several significant legal gaps.

The reasons for this are many. But I will focus much of my comments on the distortion of §230 of the Communications Decency Act which is the direct cause of an ecosystem that not only fails to protect children but incentivizes the tech industry to put them at risk and cause harm with impunity.

To adequately discuss §230 of the Communications Decency Act, two principles must frame our discussion. First, the myths surrounding the history of the purpose of §230 of the Communications Decency Act must be dispelled as the law is properly understood as a *law emerging out of a landscape of child protection*, not one seeking solely internet freedom. The second framing principle is that at the time of the debate and creation of this law, it can be consider an experiment – an experiment its proponents argued would protect children and families from exploitation and indecent content. With this framing in mind, we must then examine the results and effects of this experiment regarding exploitation and indecent content. By "result" I intend to discuss what happened to the protective law since its passage in 1996 and the campaign of the tech industry to distort it from a law of limited protection to one of de facto near absolute immunity. By "effect," I intend to discuss the massive harms this distortion causes children.

¹ E.g., **The Indecency and Injustice of the Communications Decency Act**, *Harvard Journal of Law and Public Policy*, Vol. 41, No. 2 (2018); **History Repeats Itself: The New Faces Behind Sex Trafficking Are More Familiar Than You Think**, *Emory Law Journal Online*, Vol. 68 (2019); **The Third Dimension of Victimization**, *Ohio State Journal of Criminal Law*, Vol. 13, No.1 (2016); **The Digital Nexus of Commercial Exploitation of Children and Adolescents in the United States: From the Streets to Cyberspace**, *Sexual Development, The Digital Revolution, and the Law*, Oxford University Press (Co-Author) (2014).

Here, it is apparent that the threats facing children in the digital era are profound both in their volume and severity, and that these effects did not occur by accident. Rather, they are a direct result of the tech industry actively distorting the intent of §230 of the Communications Decency Act in courtrooms across the country to transform it from a law intended to incentivize protection to one that incentivizes harmful actions by providing de facto near absolute immunity for them.

Therefore, with these framing principles and examination of the harm, there is one conclusion. This experiment of a distorted §230 of the Communications Decency Act has failed. I suggest Congress must act to remedy this and offer some principles to consider including the need to amend §230 of the Communications Decency Act and return it to its original purpose: limited immunity to protect children, not de facto near absolute immunity to harm them.

I. Principle One: Section 230 of the Communications Decency Act Emerged from a Child Protection Landscape

Section 230 of the Communications Decency Act must first be understood as a law that emerged out of a landscape of child protection. Although the tech industry and its surrogates attempt to frame it as a stand-alone provision solely to protect the Internet, that is incorrect. While that is not to say it is a “child protection statute,” it is not as it addressed multiple concerns. However, the backdrop of the discussion was protection and the structure, history and text, of the legislation reflect §230 of the Communications Decency Act emerged from a landscape of child protection.

A. The Structure of §230 of the Communications Decency Act Demonstrates It Emerged From a Child Protection Landscape

This legislation is often referred to as simply “§230.” That is a mistake as doing so can be misleading – divorcing it from its purpose. Its title and location in the U.S. Code make clear it is legislation emerging from a child protection context. The full title of § 230 is *Protection for Private Blocking and Screening of Offensive Material*. By this very title Congress was clear as to the protection intended: for blocking and screening of offensive material – not protection for disseminating harmful material. This is abundantly clear with its placement within the Communications Decency Act (CDA) which became part of the Telecommunications Act of 1996. As it updated the telecommunications legal infrastructure, Congress in its wisdom recognized that the potential for exploitive material and child abuse occurring on this new medium - without the old medium’s guardrails - was high. Therefore, as part of the Telecommunications Act, Congress directly addressed that and included the CDA within this law. If that were not clear enough, it placed the Communications Decency Act within the *Obscenity and Violence* title and the *Obscene, Harassing, and Wrongful Utilization of Telecommunications* subtitle. All these

structural efforts reflect this history and this legislation was not a stand-alone bill designed for broad immunity but one specifically targeting indecent material and exploitation.²

B. Legislative History and Contemporary Coverage of the Creation of §230 of the Communications Decency Act Demonstrate Its Emergence From a Child Protection Landscape

In 1996 Congress faced regulatory questions around “new” mediums such as cable television, digital communication, and a nascent dial up World Wide Web. It embarked on an effort to update the outdated 60 year old Communications Act of 1934. At that time Congress did not even imagine today’s Internet. In 1996 only 20% of users went online every day and the average American spent less than 30 minutes a month exploring the Internet, dial up was the main form of connection, and users numbered less than 45 million people worldwide.³ Social media was not yet the norm. Twitter, Facebook, Snap, Pornhub, Grindr, or TikTok did not exist. Regarding sexual exploitation material, the Supreme Court stated that “users seldom encounter such content accidentally. . . . ‘Almost all sexually explicit images are preceded by warnings as to the content.’”⁴

To its credit, however, many members of Congress were aware of the risks of platforms expanding explicit and harmful material, CSAM (then described as child pornography), cyberstalking, and adult sexual offenders gaining unprecedented access to children.⁵ To address these concerns, the Senate proposed a bipartisan and revised Communications Decency Act as part of the Telecommunication Act to protect children and families from indecent material.⁶ It is important to note that even those senators who opposed the CDA on other grounds, explicitly recognized the CDA was designed from a protective framework and endorsed the goal to “protect children from obscene and indecent material.”⁷ Thus, this effort to limit the spread of indecent material and protect children was shared by many and the Telecommunications Bill passed the Senate 81-18.

In the House of Representatives, two Congressmen responded to both the CDA approach to limit this material at the point of distribution and a New York state trial court defamation decision *Stratton*

² Telecommunications Act of 1996, Pub. L. No. 104, 110 Stat. 56 (1996); 47 U.S.C. 230(b)(1),(2).

³ E.g., *Reno v. A.C.L.U.*, 521 U.S. 844, 850 (1997); Farhad Manjoo, *Jurassic Web*, *Slate* (Feb. 24, 2009, 5:33 PM).

⁴ *Reno*, 521 U.S. at 853 (quoting *ACLU v. Reno*, 929 F. Supp. 824, 844 (E.D. Pa. 1996)).

⁵ 141 Cong. Rec. S1954 (daily ed. June 9, 1995).

⁶ 141 Cong. Rec. S8088 (daily ed. June 9, 1997) (comments of Sen. Exon) (“The fundamental purpose of the Communications Decency act is to provide much needed protection for children.”); *see also* 141 Cong. Rec. S8089 (“The heart and soul of the Communications Decency Act are its protections for families and children.”).

⁷ E.g., 141 Cong. Rec. S8331 (daily ed. June 14, 1995) (comments of Sen. Leahy) (endorsing the need to “keep hardcore pornography away from our children,” imprison child pornographers, but also have a functioning Internet.).

*Oakmont v. Prodigy Services Co.*⁸ Stratton Oakmont sued Prodigy for defamation regarding an anonymous post on its financial services bulletin board accusing Stratton Oakmont of fraudulent practices. In contrast to precedent and reality,⁹ this state court found Prodigy responsible for that third party content in part because of Prodigy's active screening out of inappropriate material.¹⁰ The court considered Prodigy a publisher of the information under state law because "it voluntarily deleted some messages . . . and was therefore legally responsible for the content of defamatory messages that it failed to delete."¹¹ Counterintuitively, the trial court held Prodigy responsible for the post because it attempted to monitor its board while in previous cases similarly situated platforms were not considered publishers of such third party content.¹² Notwithstanding that this was a singular state level opinion, two members of the House were concerned about the implication of that case on the CDA's framework of stopping material at the point of distribution. Within the context of the child protection debate that the CDA began, these congressmen proposed the Internet Freedom and *Family Empowerment Act* of 1995 (IFFE)(emphasis added). As the name suggests, this bill was concerned with both internet issues but also in *protecting families*, not in protecting platforms. The debate was never *whether* to limit indecent material and shield families, but *how* to do so effectively.

Therefore, among other goals, IFFE did not want to disincentivize a company from monitoring its platforms for improper third party content by having them face liability for doing so.¹³ A backdrop of the discussion with this bill was legislating the most effective method to limit indecent and harmful material. The IFFE approach was attached to the House version of the Telecommunications bill.

The Telecommunications bills went into committee negotiations with two different versions on how to address indecent material and protect children. The first from the Senate, the CDA, acknowledged

⁸ No. 31063/94, 1995 WL 323710, *2 (N.Y. Sup. Ct. 1995); *contra*, *Cubby, Inc. v. Compuserve, Inc.*, 776 F.Supp. 135 (SDNY) (Dismissing defamation action against defendant who sold access to library of news publications because defendant was a mere distributor and not a publisher.)

⁹ Ironically, the leadership of Stratton Oakmont pled guilty to stock manipulation occurring during this time. Edward Wyatt, Stratton Oakmont Executives Admit to Stock Manipulation, New York Times (Sept. 24, 1995).

¹⁰ No. 31063/94, 1995 WL 323710, *2 (N.Y. Sup. Ct. 1995); *contra*, *Cubby, Inc. v. Compuserve, Inc.*, 776 F.Supp. 135 (SDNY) (Dismissing defamation action against defendant who sold access to library of news publications because defendant was a mere distributor and not a publisher.)

¹¹ Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1163 (9th Cir. 2008) (citing *Stratton Oakmont v. Prodigy Servs. Co.*, 1995 WL 323710, *4 (Sup. Ct. May 24, 1995)).

¹² *Stratton Oakmont v. Prodigy Servs. Co.*, 1995 WL 323710 (Sup. Ct. May 24, 1995); *see also* Doe v. AOL, 783 So. 2d 1010, 104 (2001) (citing Steven M. Cordero, Comment, *Domnum Absque Injuria*, Zeran v. AOL: Cyberspace Defamation Law, 9 FORDHAM INTELL. PROP., MEDIA AND ENT. L.J. 775 (1999)).

¹³ Christopher Cox, *The Origins and Original Intent of Section 230 of the Communications Decency Act*, UNIV. RICH. J. L. AND TECH., 64 (2020) (Its sponsor has also argued it was important to respond to Stratton Oakmont because "common law extended no protections to platforms that moderate user content."); *Stratton Oakmont v. Prodigy Servs. Co.*, 1995 WL 323710, *1 (Sup. Ct. May 24, 1995).

the value of the Internet¹⁴ but also prioritized shielding children and families from explicit content and ensuring it would not facilitate child abuse and exploitation. The IFFE, while respecting the concerns of the CDA, sought, *inter alia*, to incentivize platforms to monitor their sites promising this would protect children and families. It is critical to understand the text of Section 230 of the Communications Decency Act of today emerged from this landscape of protection.

Following months of negotiation, the final Telecommunications Act of 1996 struck parts of IFFE but embraced both approaches to protecting children by including parts of the text of the IFFE within the CDA under Section 230. By placing the protective language of IFFE into §230 of the CDA, this statute must be read as being anchored in shielding families from indecent materials by incentivizing platforms to do just that.

Although the technology industry, their surrogates, and even authors of the IFFE at times try to divorce Section 230 from these roots, that is how it was situated within the law as it emerged from Conference and how it was passed by Congress. Contemporary Congressional debate around the legislation reflects that Title V- which housed this small language from the IFFE concepts as a component of the CDA – reflects this child protection landscape.¹⁵ Obviously, the 107 pages of the Telecommunication Act of 1996 had many goals.¹⁶ But Congress made clear by including §230 of the CDA within the Obscenity and Violence Title that this Section possesses child protection elements.¹⁷ Chief Judge Katzmann described this history of Section 230 by noting that,

¹⁴141 CONG. REC. S8089 (daily ed. June 9, 1995) (comments Sen. Exon) (“The computer is a wonderful device for arranging, storing, and making it relatively easy for anyone to call up information or pictures on any subject. That is part of the beauty of the Internet system.”).

¹⁵ When the Senate was actually debating the Conference Report, one Senator noted that “the Internet indecency provisions have met with the barest of resistance in this Chamber.”; 142 Cong. Rec. 1993, 2036 (comments of Sen. Feingold).

¹⁶142 CONG. REC. 1993, 2041 (comments of Sen. Exon) (“Concurrent with our efforts to make the Internet and other computer services safe for families and children, this bill includes legislation which will help turn the information revolution to the benefit of all Americans, but especially America’s children.”); “a needed step in protecting children from child molesters and unscrupulous porn merchants,” noting the need for federal legislation in this area, not just new technologies. 142 CONG. REC. 1993, 2041.

¹⁷ *E.g.*, 142 CONG. REC. 1993, 2013 (comments of Sen. Stevens) (noting this is not a deregulation bill); *see also, id.* at 2030 (comments of Sen. Coats) (“Perhaps most importantly this bill will help protect children from computer pornography which today is readily accessible on the internet.”). One Senator noted that “the Conference Report contains strong protections for America’s children.” 142 Cong. Rec. 1993, 2030 (comments of Sen. Holmes); 142 Cong. Rec. 1993, 2030 (comments of Sen. Coats)(noting the linkage between the bill and protecting children from not only pornography but “images and text dealing with the sexual abuse of children.”). Although there were opponents to the bills, the framing of its protective purpose was not in dispute. *E.g.*, 142 Cong. Rec. 1993, 2015 (comments of Sen. Leahy)(acknowledging that “[a]ll of us 100 members of the U.S. Senate oppose the idea of child pornography,” but expressing constitutional concerns about two provisions of the CDA outside §230); 142 Cong. Rec. 1993, 2035 (comments of Sen. Feingold)(discussing the legislation as redundant to current federal laws regarding child abuse, stating that “much of what the proponents of this legislation wish to banish from cyberspace

[o]f the myriad of issues the emerging Internet implicated, Congress tackled only one: the ease with which the Internet delivers indecent and offensive material, especially to minors....The Conference Committee had two alternative versions for countering the spread of indecent online material to minors. The Committee chose not to choose. Congress instead adopted both amendments as part of the final Communications Decency Act.¹⁸

Congress viewed §230 of the Communications Decency Act as a tool in the toolbox of combatting indecent material and protecting children, as well as protecting platforms from liability for efforts to do so themselves.

C. The Text Itself Demonstrates §230 of the Communications Decency Act Emerged From a Child Protection Landscape

Although it has since been distorted by the tech industry, the plain language of §230 of the Communications Decency Act explicitly underscores this child protection backdrop. An example is Congress’s naming of the section “Protection for Private Blocking and Screening of Offensive Material.” The word “protection” is important but more important is the explicit statement for what a platform would receive protection: blocking and screening of offensive material not for failing to do so or for facilitating such material. Notably, the word “immunity” is absent. From this text.

Congress included five statements of the policy of the United States. Three policies speak to the protective intentions behind the bill.¹⁹ Among those, the statute explicitly states that it is the policy of the United States to “ensure vigorous enforcement of Federal criminal laws to deter and punish *trafficking in obscenity, stalking, and harassment by means of [a] computer*”—the very concerns mentioned in the CDA debates. The inclusion of these policies, combined with the text of the provision that explicitly states the statute should have no effect on enforcement of obscenity and child exploitation federal criminal law, reflect the climate from which § 230 came: a discussion about the best methods to protect children from explicit material and exploitation.

Critical to the supporters of the IFFE, § 230 of the Communications Decency Act includes language providing what was intended to be limited protection for platforms. As the title of §230 of the Communications Decency Act suggests, the protection includes protection from civil liability for “Good Samaritan” blocking or screening of offensive material made in good faith. Congress explained “offensive material” is “material that the provider or user considers to be obscene, lewd, lascivious,

is already subject to criminal penalties – obscenity, child pornography, and child exploitation via computer networks are already criminal acts.”) Those who opposed the CDA did so on other constitutional grounds unrelated to §230 of the CDA which were resolved in *Reno v. ACLU*, 521 U.S. 844, 874 (1997).

¹⁸*Force v. Facebook*, 934 F.3d 53 (2d Cir. 2019) (Katzmann, CJ dissenting). Chief Justice Katzmann also rejected the argument that Section 230 had nothing to do with the CDA and observed that its placement within the CDA was not coincidence.

¹⁹ 47 U.S.C. §230(b).

filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.”²⁰

Not only does this provision reflect the clear intent of Congress to offer limited protection to platforms, it confirms the protection from civil liability is related to child and family protection. The other protection from liability is located in §230(c)(1) and describes not treating platforms as publishers. “Looking at the text... §230(c)(1) does not ‘declare a general immunity from liability deriving from third-party content.’ Indeed, §230(c)(1) ‘does not mention ‘immunity’ or any synonym.’”²¹ Rather, ICSs were protected only from publisher liability—not distributor liability. “*Stratton Oakmont*’s rule created a perverse incentive not to moderate any offensive content, and Congress was concerned. So, in 1996, Congress enacted 47 U.S.C. § 230 [and] ... was meant to bring traditional “distributor” immunity online.”²² To read it otherwise is manufactured. As Justice Thomas noted, “[i]t is odd to hold, as courts have, that Congress implicitly eliminated distributor liability in the very Act in which Congress explicitly imposed it.”²³

Furthermore, the legislation explicitly states that it will not affect the enforcement of any criminal statute, but also specifically mentions not impacting laws relating to obscenity and the sexual exploitation of children.²⁴ This text reflects many priorities, and explicitly includes child protection. The Report’s discussion concerning the CDA and IFFE’s goals of developing the most effective methods to protect children supports the plain language understanding of the text. The Conference Report states:

This section [§ 230] provides “Good Samaritan” protections from civil liability for providers or users of an interactive computer service for actions to restrict or to enable restriction of access to objectionable online material. . . . The conferees believe that such decisions [similar to *Stratton Oakmont*] create serious obstacles to the important federal policy of empowering parents to determine the content of communications their children receive through interactive computer services.²⁵

Therefore, as a framing principle, §230 of the Communications Decency Act must be understood not as a stand-alone bill asserting broad immunity, but as a narrow bill (albeit with multiple goals)

²⁰ 47 U.S.C. §230(c)(2).

²¹ *Calise v. Meta Platforms, Inc.*, 103 F.4th 732, 740 (9th Cir. 2024)(quoting *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1100 (9th Cir. 2009) and *Chi. Lawyers’ Comm for Civ. Rts. Under Law, Inc. v. Craigslist*, 519 F.3d 666, 669 (7th Cir. 2008).

²² *Calise*, 103 F.4th at 739. See also ²² *Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC*, 141 S. Ct. 13, 14-15 (2020) (mem.).

²³ *Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC*, 141 S. Ct. 13, 14-15 (2020) (mem.).

²⁴ 47 U.S.C. §230(e).

²⁵ Telecommunications Act of 1996, S. Rep. No. 104-230, at 194 (1996) (emphasis added).

emerging out of a landscape of protection from child exploitation and harm. This is supported by the structure, history, and text of the legislation.

II. Principle Two: The IFFE Provisions Were Effectively An Experiment Based Upon the Promise That if Included They Would Be the Strongest Way to Protect Children and Families

The second framing principle is that the current text of the §230 of the Communications Decency Act was offered as an experiment and that has failed. Whether analyzing the forces behind the IFFE or the support for the final version of §230 of the Communications Decency Act it is essential to understand the basic promise proponents made in including §230(c)(1). They promised that these provisions would be the most effective way to protect children and shield explicit conduct because read together §230(c)(1) and (c)(2) would incentivize platforms to monitor and prevent this content. However, the way in which §230 of the Communications Decency Act has been distorted, it has not.

That is to say that the final text of the §230 of the Communications Decency Act was Congress accepting the invitation of the proponents of the IFFE and the tech industry to experiment that (c)(1) would be protective. Critically, companies argued that such an approach encouraged, indeed promised, that tech companies would produce workable technologies that would allow parents and users to filter out such material.²⁶

By incorporating parts of the IFFE into the CDA, Congress prohibited both the illegal transmission of such material, but also accepted the industry's promise that it would utilize the incentive to develop parental controls and filters and provide them to the public.²⁷ Additionally, this was the vision of IFFE proponents who argued that both federal law and technological solutions were needed to protect children.²⁸ This was the experiment: a twofold approach with narrow limited liability for efforts to protect children would lead to a safe internet. Although that technology did not exist, the tech industry happily promised it would develop it and it would become more sophisticated and easily available to parents.²⁹

²⁶ Steve Lohr, Conservatives Split on How to Regulate the Internet, N. Y. Times, Nov. 9, 1995, at D4 (“Both camps agree on the need to protect children from offensive material on computer networks. But the methods they advocate represent two divergent views on how to regulate the fast-growing medium.”).

²⁷ Nicolas Conlon, Freedom to Filter Versus User Control: Limiting the Scope of § 230(C)(2) Immunity, 2014 Univ. Ill. J. L. Tech. & Pol’y 105, 115.

²⁸ See Kara Swisher, Ban on On-Line Smut Opposed, Wash. Post, July 18, 1995, at D3 (describing how the tech industry and law makers worked on a compromise, including the consideration of several proposals, such as replacing the term “indecent” to “harmful to minors” and implementing credit card verification as a means of restricting access).

²⁹ Robert Corn-Revere, New Age Comstockery, 4 Comm. L. Conspectus 173 (1996).

Contemporary news accounts demonstrate the tech companies' false promises about the ability of what would become § 230 to protect children.³⁰ These representations were not inconsequential but a component of an intensive lobbying effort to embrace this experiment.³¹ The *Washington Post* described how "[o]n-line companies, software makers and civil liberties groups came to Capitol Hill yesterday to make their case that the on-line world can be made safe for children without government intervention."³² The result of this effort was characterized as one in which some "reject[ed] promises from the on-line industry that companies like [AOL] and Netscape Communications Corp. would give parents tools to screen offensive material if they could be sure such actions wouldn't make them liable for any message sent by any subscriber."³³ The rejection of this promise was prophetic. The Department of Justice studied the effects of § 230, concluding that this "expansive statutory interpretation, combined with technological developments, has reduced the incentives of online platforms to address illicit activity on their services."³⁴ Moreover, the public has not seen the type of screening or parental controls suggested. While the tech industry argues that it does provide controls,³⁵ a common chorus is that they are neither effective, nor readily accessible.³⁶ That is exactly the opposite of what the §230 proponents promised.

Congress intended this statute to provide limited protection to platforms based on their representation that such immunity would empower platforms to protect children and families. This experiment has failed because the tech industry has replaced limited liability with de facto near absolute immunity.³⁷ As the Ninth Circuit noted, "when an internet company has an economic incentive to permit

³⁰ The *Washington Post* reported that tech companies promised to provide and utilize technology to filter out such material. Kara Swisher & Elizabeth Corcoran, *Gingrich Condemns On-Line Decency Act*, *Wash. Post*, June 22, 1995, at D8.

³¹ The *New York Times* reported that "Interactive Services Association, a trade group for the on-line industry that supports the Cox-Wyden Amendment," demonstrated for the staff members of the conferees on the telecom bill "software that can filter out material deemed objectionable. Lohr, *supra* note 26.

³² *E.g.*, Swisher, *supra* note 28, at D3.

³³ Daniel Pearl, *Compromise Sought on Curbs for the Internet: On-Line Service Firms Seek to Check Harsh Rules on Controlling Content*, *Wall St. J.*, Dec. 4, 1995, at B8.

³⁴ *Department of Justice's Review of Section 230 of the Communication Decency Act Of 1996*, Dep't. of Just. Archives, <https://www.justice.gov/archives/ag/departments-justice-s-review-section-230-communications-decency-act-1996>.

³⁵ *E.g.*, *Our Tools, Features and Resources to Help Support Teens and Parents*, Meta, <https://www.meta.com/help/policies/safety/tools-support-teens-parents/> [<https://perma.cc/2AFG-ZJ6U>] (Dec. 2024).

³⁶ *E.g.*, Brian Fung & Clare Duffy, *Kids Aren't Safe on Social Media, Lawmakers Say: Tech CEOs Are Back in DC to Pledge (Again) that They'll Handle It*, *CNN Bus.* (Jan. 29, 2024, 6:42 PM), <https://www.cnn.com/2024/01/29/tech/big-tech-ceos-youth-safety-senate-testimony/index.html> [<https://perma.cc/66J3-M4QC>]; Tatum Hunter, *Instagram's New Teen Safety Features Still Fall Short*, *Critics Say*, *Wash. Post* Jan. 10, 2024; IWF, *Meta Failing to Stop Spread of Sexual Abuse Imagery In the Wake of the Huw Edwards Scandal* (Aug. 16, 2024).

³⁷ The OSCE studied global laws and that a system of allowing self-regulation has largely failed. OSCE, *Policy Responses to Technology-Facilitated Trafficking in Human Beings* (2022).

unlawful content to be posted by third parties, it seems to encourage the opposite [of self-regulation] – willful blindness.”³⁸

III. The Result of this Failed Experiment Is De Facto Near Absolute Immunity

As will be discussed in Section IV, that §230 of the Communications Act failed to protect children and families from exploitation and indecent content is beyond dispute. Statistics from NCMEC, Interpol, Internet Watch and others all underscore the harms of exploitive content delivered to children on tech’s platforms.³⁹ Had the language of §230 of the Communications Decency Act been adhered to, it is possible that the concept of limited protection from civil liability for Good Samaritans would have provided the incentive to create a protective regime. But it did not. In large part because after making such promises, those tech companies embarked on an effort to expand this immunity. They did so by advocating in courtrooms across America for an interpretation of § 230 providing much broader immunity than legislators intended or the text reflected, and caused its expansion far beyond its original purpose.

This began with the very first published opinion, *Zeran v. America Online*.⁴⁰ In this defamation case, the Fourth Circuit focused on the policies of §230 of the Communications Decency Act relating to limited regulation, but ignored the numerous other policies regarding protections from indecent material.⁴¹ Its language characterizing §230 of the Communication Decency Act as “broad” took on a life of its own in subsequent cases. Recently, however, more judges have been calling for a return to the text and for Congress acknowledged to correct it.⁴²

With tech companies and their surrogates throughout the country seizing on this language, many courts have accepted this early characterization as true, and, instead of quoting from the text of the legislation, quoted heavily from *Zeran*, notwithstanding the textual and historical record. These include

³⁸ Calise, 103 F.4th at 747 (Nelson, J. concurring).

³⁹ Interpol & ECPAT Int’l, **Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material: Summary Report 1** (2018); Internet Watch Found., **WF Annual Report 2023 #Behind the Screens**, (2023); Department of Justice Press Release, **FBI and Partners Issue National Public Safety Alert on Sextortion Schemes** (Jan. 19, 2023); NCMEC, **2023 Cybertipline Report** (2024).

⁴⁰ *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997).

⁴¹ *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997). At one point the Fourth Circuit did acknowledge that “Section 230 was enacted, *in part*, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum.” *Id.* However, it never explained the other purposes of §230 which demonstrate the very limited immunity and that qualifier has largely been ignored.

⁴² *E.g.*, *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1163 (9th Cir. 2008); *Jane Doe #1 v. MG Freesites, Ltd.*, No. 7:21-cv-00220-LSC, 2022 U.S. Dist. LEXIS 23199 (N.D. Ala Feb. 9, 2022); *Doe v. Am. Online*, 783 So. 2d 1010, 1019 (Fla. 2001) (Lewis, J. in dissent); *Calise v. Meta Platforms, Inc.*, 103 F.4th 732, 740 (9th Cir. 2024); *Doe v. Snap, Inc.*, 88 F.4th 1069, 1070 (5th Cir. 2023) (per curiam) (Elrod, J., dissenting from denial of reh’g en banc) (describing the interpretation as “sweeping immunity for social media companies that the text cannot possibly bear.”)

an early case finding immunity for a civil allegation that a platform distributed CSAM, allowed advertisements for CSAM, and a failed to respond to notification that its services were being utilized to distribute obscene material.⁴³ In *Doe v. America Online*, the dissent was clear:

Contrary to the majority's view, however, the carefully crafted statute at issue, undergirded by a clear legislative history, does not reflect an intent to totally exonerate and insulate an ISP from responsibility where, as here, it is alleged that an ISP has acted as a knowing distributor of material leading to the purchase, sale, expansion and advancement of child pornography ⁴⁴

The concerns of the dissent in that case prophetically forewarned this would create “carte blanche immunity for wrongful conduct plainly not intended by Congress.”⁴⁵

This concerted effort by tech companies to argue for broader immunity – notwithstanding the intent of §230 of the Communications Decency Act, has turned the provision on its head. Rather than a shield for preventing harm, they have successfully distorted it to shield for facilitating or creating harm. Examples include near de facto near absolute immunity for claims of creating algorithms that facilitate and spread terrorism,⁴⁶ refusing to follow court orders,⁴⁷ advertising and engaging illegal firearms sales,⁴⁸ designing dating app without safety features to protect users from known dangerous conduct on its platforms including allowing other users to impersonate plaintiff and direct others to plaintiff's home for sex;⁴⁹ knowingly designing, managing, and promoting an app to be used to groom and sexually abuse minors;⁵⁰ facilitating sex trafficking,⁵¹ creating a tool for reprogramming a computer system for cars and provided technical assistance and guidance on using the tool to defeat emission controls,⁵² to name a few. One recent example is *Doe v. Webgroup Czech Republic*.⁵³ Here, the trafficked plaintiff accused defendants of knowingly receiving videos of her sexual exploitation, which were CSAM because she was a child.⁵⁴ Defendants claimed § 230 immunity for the receipt and possession of CSAM. Importantly,

⁴³ *Doe v. Am. Online*, 783 So. 2d 1010 (Fla. 2001).

⁴⁴ *Doe v. Am. Online*, 783 So. 2d 1010, 1019 (Fla. 2001)(Lewis, J., dissenting).

⁴⁵ *Doe v. Am. Online*, 783 So. 2d 1010, 1019 (Fla. 2001) (Lewis, J. dissenting).

⁴⁶ *Force v. Facebook*, 934 F.3d 53 (2d. Cir. 2019).

⁴⁷ *Hassell v. Bird*, 420 P.3d 776, 789 (Cal. 2018) (Yelp's refusal to comply with a court injunction is protected by Section 230).

⁴⁸ *Daniel v. Armslist, LLC*, 926 N.W.2d 710, 715, 726 (Wis. 2019), cert. denied, 140 S.Ct. 562 (2019) (website was immune under Section 230, despite allegations that website intentionally designed to evade federal firearm laws).

⁴⁹ *Herrick v. Grindr LLC*, 765 F. App'x 586 (2d Cir. 2019)

⁵⁰ *Doe v. Snap, Inc.* 2022 WL 2528615 (S.D. TX July 7, 2022), aff'd by 2023 WL 4174061, (5th Cir. June 26, 2023), re'h en banc den'd by 88 F.4th 1069 (5th Cir. Dec. 18, 2023).

⁵¹ *Doe v. Backpage.com, LLC*, 817 F.3d 12, 16-21 (1st Cir. 2016). Plaintiffs – sex trafficking survivors who were repeatedly sold on Backpage.com, accused defendants of entering into a joint venture with sex traffickers wherein Backpage adapted posting requirements, accepted anonymous payments, advised traffickers how to avoid law enforcement, and stripped images of metadata – all to facilitate sex trafficking. *Id.*

⁵² *United States v. EZ Lynk, et.al*, 2024 WL 1349224 (S.D. N.Y. March 28, 2024).

⁵³ No. 21-CV-02428, 2024 WL 3533426 (C.D. Cal. July 24, 2024).

⁵⁴ *Id.* at *6.

receipt and possession of CSAM is a federal crime, and Congress has made it also a basis for a private right of action.⁵⁵ Notwithstanding that, the district court accepted the platforms argument and found that:

[I]nsofar as Plaintiff seeks to hold Defendants liable for “receipt” of the illicit [CSAM] videos, these claims are immune from liability under Section 230. Receipt of materials or content is, as it were, simply the first step in any publishing regime; if so, then mere receipt of illicit [CSAM] material is not sufficient to preclude immunity under Section 230.⁵⁶

This court essentially concluded that § 230 immunizes a platform for acts that explicitly federal criminal law. Clearly, that is not the intent behind § 230’s text, purpose, or history.

None of these actions remotely resemble traditional publishing duties or Good Samaritan removal of objectionable content. Yet, citing to the very early § 230 cases from the early 2000’s, these courts found these platforms immune from prosecution, thereby denying victim survivors the opportunity to prove their case. One judge described courts’ actions as follows:

[F]rom the very start, courts held § 230 did much more than overrule Stratton Oakmont’s publisher-liability theory. . . . Though Zeran has been criticized as inconsistent with the text, context, and purpose of § 230 . . . , the opinion was cut-and-paste copied by courts across the country in the first few years after the statute arrived.⁵⁷

Calling the current jurisprudence a “*far cry* from what has prevailed in court” Justice Thomas lamented the “too-common practice of reading extra immunity into statutes where it does not belong... to grant sweeping protections to Internet platforms.”⁵⁸ Of particular concern to Justice Thomas was the trend in courts departing from Section 230 text. “Courts have done so by awarding immunity for their own content in contrast to Section 230(c)(1) and eviscerating the narrower liability” of Section 230(c)(2)(A).⁵⁹ He has referred to platforms abuse of this provision as “[s]ocial-media platforms have increasingly used § 230 as a get-out-of-jail free card.”⁶⁰ Similarly, this reality caused the Department of Justice to note that “the combination of significant technological change since 1996 and the expansive interpretation that

⁵⁵ 18 U.S.C. §§ 2252, 2255 (2024).

⁵⁶ WebGroup Czech Republic, 2024 WL 3533426, at *6.

⁵⁷ Anderson v. Tiktok, Inc., 116 F.4th 180, (3d Cir. 2024)(Matey J. concurring in part dissenting in part)(emphasis added).

⁵⁸ Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 4, 7(2020) (citations omitted).

⁵⁹ Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 7, 8, 10 (2020) (citing to Doe v. Backpage.com, LLC, 817 F.3d 12, 16-21 (1st Cir. 2016); M.A. v. Vill. Voice Media Holdings, 809 F.Supp.2d 1041, 1048 (E.D. Mo. 2011); Doe v. Bates, No. 5:05-CV-91-DF-CMC, 2006 WL 3813758, *18 (E.D. Tex., Dec. 27, 2006). Even after Justice Thomas’ insights, tech has argued and some courts have agreed - refusing to look more closely at the articulated purposes of §230 of the CDA. Instead of self-correcting the widely held belief that the current breadth of the immunity exceeded the intent of Congress, courts have claimed too many companies rely on this broad interpretation and they do not want to upset this reliance. In re Facebook, 625 SW.3d 80, 91-93 (Tex. 2021); Daisuke Wakabayashi, *Legal Shield for Social Media Targeted By Lawmakers*, N. Y. TIMES (May 28, 2020), <https://www.nytimes.com/2020/05/28/business/section-230-internet-speech.html>. This is a stunning statement given that “the Internet industry has a financial incentive to keep Section 230 intact.” Id.

⁶⁰ Doe v. Snap, Inc., 144 S. Ct. 2493, 2494 (2024) (Thomas, J., dissenting denial of certiorari) (mem.).

courts have given §230...has left online platforms immune for a wide array of illicit activity on their services.”⁶¹

IV. The Effect of This Conscious Effort of the Tech Industry to Distort §230 of the Communications Decency Act Is Profound

The above section discussed the *result* of the §230 experiment – de facto near absolute immunity. This section discussed the *effect* of that immunity on people and on our legal systems

A. The Harm Caused to Individuals By De Facto Near Absolute Immunity Far Exceeds Congress’ Worst Fears n 1996

The Senate Judiciary Committee is familiar with the statistics regarding the effect of de facto near absolute immunity and this distortion of §230 of the Communications Decency Act. Just considering CSAM, the following is indicative of the scope of the harm. Twenty-nine years after the passage of Section 230, the fears of the Senate regarding what the Intern *could* become have not only been realized, but surpassed. Focusing on CSAM alone, this illegal material is monetized and amplified by several of these platforms who do so with impunity. This evident in a review of reports to the CyberTipline. In 1998, when the CyberTipline opened it had approximately 4500 reports.⁶² In 2023 the Senior Vice President for NCMEC testified before the House Oversight Committee as follows:

In 2022, NCMEC received over 32 million reports and more than 88 million pieces of content. Last year, NCMEC received more than 36 million reports containing more than 105 million pieces of content. Since its inception over 25 years ago, the CyberTipline has received more than 186.2 million reports containing more than 530.8 million images, videos, and other content relating to child sexual exploitation. Currently, NCMEC receives on average more than 99,000 CyberTipline reports every day.⁶³

In the recent years, video depictions of child sexual exploitation outpace still images of this material.⁶⁴ Their content is violent and an Interpol study found more than 60% of the images of identified children

⁶¹ *Department of Justice’s Review of Section 230 of the Communication Decency Act Of 1996* (2020), Dep’t. of Just. Archives, <https://www.justice.gov/archives/ag/departments-justice-s-review-section-230-communications-decency-act-1996>.

⁶² Statement of Yiota Souras, Sr. Vice President, National Center for Missing and Exploited Children, EARN IT Act Press Conference, February 18, 2022.

⁶³ Testimony of John Shehan, Sr. Vice President, National Center for Missing & Exploited Children United States House Committee on Oversight and Accountability Subcommittee on Cybersecurity, Information Technology, and Government Innovation, “Addressing Real Harm Done by Deepfakes,” March 12, 2024.

⁶⁴ Statement of Yiota Souras, Sr. Vice President, National Center for Missing and Exploited Children, EARN IT Act Press Conference, February 18, 2022. These trends are echoed by the Canadian Centre for Child Protection, which in 2017 averaged approximately 4000 tips per month, 98% of them being child sexual abuse imagery.; Canadian Centre for Child Protection, *Survivor’s Survey, Executive Summary* at 1 (2017).

were prepubescent children including infants and toddlers.⁶⁵ The Department of Justice discussed the harms of being depicted in CSAM:

When these images are placed on the Internet and disseminated online, the victimization of the children continues in perpetuity. Experts and victims agree that victims depicted in child pornography often suffer a lifetime of re-victimization by knowing the images of their sexual abuse are on the Internet forever. The children exploited in these images must live with the permanency, longevity, and circulation of such a record of their sexual victimization. This often creates lasting psychological damage to the child, including disruptions in sexual development, self-image, and developing trusting relationships with others in the future.⁶⁶

This is echoed by survivors themselves who discuss that CSAM affects them differently than child sexual abuse, pointing to “permanence of the images and the fact that if the images are distributed, their circulation will never end.”⁶⁷

B. The Harm Caused By De Facto Near Absolute Immunity To Society and Access to Justice Is Profound

Two additional effects of de facto near absolute immunity must be noted and both relate to the courts. The first is the capacity for harm an unregulated industry possesses when those they harm do not have access to the courts. The second is the uniquely pernicious harm preclusion of discovery has for victims and society.

First, this distortion of Congressional intent with the Communications Decency Act and the undermining of Congressional action regarding trafficking, CSAM, and other forms of exploitation has shut the courthouse door to victims, states attorneys general, and others harmed. Importantly, to say that these groups are shut out of the justice system is not say they are precluded from winning at trial. They are stopped from ever being able to have their day in court because the tech industry has transformed §230 of the Communications Decency Act into a de facto near absolute immunity provision, allowing for dismissal of these causes of action at the motion to dismiss stage – prior to discovery. As Justice Thomas noted,

Paring back the sweeping immunity, courts have read into §Section 230 would not necessarily render defendants liable for online misconduct. It simply would give plaintiffs a chance to raise their claims in the first place. Plaintiffs still must prove the merits of their cases, and some claims

⁶⁵ Interpol & ECPAT Int’l, **Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material: Summary Report** (2018)

⁶⁶ Child Pornography, U.S. Dep’t of Just., <https://www.justice.gov/criminal-ceos/child-pornography> [https://perma.cc/3M3X-BYMQ] (Aug. 11, 2023).

⁶⁷ **Captured on Film: Survivors of Child Sex Abuse Material Are Stuck in a Unique Cycle of Trauma**, Nat’l Ctr. for Missing and Exploited Child. 3 (2019).

will undoubtedly fail. Moreover, states and the federal government are free to update their liability laws to make them more appropriate for an Internet-driven society.⁶⁸

Part of the architecture of anti-exploitation efforts include attacking CSAM and trafficking on multiple fronts: prevention, protection, and disruption. This requires the use of criminal, civil, federal, and state tools. When companies are aware their behavior could expose them to risk of accountability, they will be deterred from illegal behavior prior to the abuse or exploitation taking place. But if, as here, they know they will never have to account for their actions, they will continue the behavior with impunity.

This is not only an injustice to individual victim survivors. Section 230 of the Communications Decency Act has been used to preclude state court prosecutions,⁶⁹ civil suits as part of statute's guaranteed private rights of action,⁷⁰ product liability civil suits,⁷¹ and federal attempts to enforce federal regulations.⁷² This is an affront to states' rights to enforce their own criminal laws, citizens' civil rights of citizens, and the right of the public to be safe from exploitative harm. Indeed, nearly all the nations attorneys' generals have come together to three times to urge Congress to amend § 230 of the Communications decency Act to allow states to enforce their criminal laws. Their recent letter noted that

Stories of online black market opioid sales, ID theft, deep fakes, election meddling, and foreign intrusion are now ubiquitous....Current precedent interpreting the CDA, however, continues to preclude states and territories from enforcing their criminal laws against companies that, while not actually performing these unlawful activities, provide platforms that make these activities possible. Worse, the extensive safe harbor conferred to these platforms by courts promotes an online environment where these pursuits remain attractive and profitable to all involved, including the platforms that facilitate them.⁷³

The second effect is what I label the **dual danger** of de facto near absolute immunity. This industry whether it be a large company or one small actor, has the capacity to cause immeasurable harm. But, notwithstanding the risk to the public welfare or individuals, it operates without any guardrails from any outside entity. In such an ecosystem, rather than being incentivized to act as a Good Samaritan, it is actually incentivized to act in a harmful manner because it has de facto near absolute immunity for its actions. Even a small company can cause tremendous damage through facilitating CSAM, human

⁶⁸ *Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC*, 141 S. Ct. 13, 9-10 (2020); For a discussion of how the tech industry actively thwarted enforcement of criminal sex trafficking laws, state development of civil and criminal liability for online sex trafficking, and victim survivor civil suits, see Mary Graw Leary, *History Repeats Itself: The Faces Behind Sex Trafficking are More Familiar Than You Think*, 68 EMORY L. J. ONLINE 1083 (2019).

⁶⁹ *E.g.*, *Dart v. Craigslist, Inc.*, 665 F. Supp. 2d 961, 967-68 (N.D. Ill. 2009).

⁷⁰ *E.g.*, *M.A. v. Vill. Voice Media Holdings*, 809 F.Supp.2d 1041, 1048 (E.D. Mo. 2011);

⁷¹ *E.g.*, *Anderson v. TikTok*, 637 F.Supp.3d. 276 (2022), rev'd 116 F.4th 180. (3d Cir. 2024).

⁷² *E.g.*, *United States v. EZ Lynk, et.al*, 2024 WL 1349224 (S.D. N.Y. March 28, 2024).

⁷³ <https://www.naag.org/policy-letter/state-ags-support-amendment-to-communications-decency-act/>

trafficking,⁷⁴ sextortion,⁷⁵ and non-consensual sexualized images.⁷⁶ With the emergence of artificial intelligence sexualized images of children and adults, the moral hazard risks are even greater.⁷⁷ Citron and Wittes convincingly note that a historical pattern exists of nascent industries beginning with no regulation but when they grow to maturity having natural guardrails in place.⁷⁸ When industries, such as transportation, utilities, and agriculture, reach a point where they can cause serious harm to large numbers of people, some form of outside oversight occurs.⁷⁹ Here with this industry, that has not occurred. Indeed, the tech industry seeks wider immunity.⁸⁰

This is a dual danger because the risk is not only the lack of guardrails for a very powerful industry. Due to the preclusion of discovery on an industry with no oversight or guardrails, the tech industry has been able to prevent the public from learning anything about its internal workings. Undoubtedly the reason the tech industry so aggressively protects the distorted immunity is that it prevents litigants from being able to prove their cases or the public from being aware of the level of their behavior. The few occasions the public has been able to learn of partnerships between platforms and exploiters was through Congressional investigations and whistleblower.⁸¹ This dual danger leaves the most vulnerable with no protection and no remedy for harm experienced due to the actions of an industry with de facto near absolute immunity from accountability. Furthermore, by precluding discovery it leaves those seeking to do harm anonymously and those platforms with immunity without limits to engage in behavior without limits.

⁷⁴ E.g., *Backpage.com's Knowing Facilitation of Online Sex Trafficking: Hearing Before the Subcomm. on Investigations*, 115th Cong. (2017); Global Report on Trafficking in Persons 2020, UNODC (referring to traffickers' use of the Internet "digital hunting fields." Katie McQue and Mei-Lin McNamara, *How Facebook and Instagram Became Marketplaces for Child Sex Trafficking*, *The Guardian* (April 27, 1993).

⁷⁵ E.g., *By The Numbers*, NCMEC (noting in 2023 the CyberTipline received 186,819 reports of online enticement which includes sextortion, and increase of 323% since 2021), available at <https://www.missingkids.org/theissues/sextortion#:~:text=digital%20dediting%20tools,-By%20the%20Numbers,enticement%20reports%20increased%20by%20323%25>.

⁷⁶ E.g., Amanda Lenhard, et.al, *Nonconsensual Image Sharing: One in 25 Americans Has Been A Victim of Revenge Porn*, *Data and Society* at 5 (Dec. 13, 2016);

⁷⁷ *How AI Is Being Abused to Create Child Sexual Imagery*, Internet Watch Foundation (Oct. 2023), available at <https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/>.

⁷⁸ Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 *Fordham L. Rev.* 401, 406 (2017)..

⁷⁹ *Id.*

⁸⁰ In 2024 tech companies continued to attempt to expand their already de facto near absolute immunity. *Calise v. eta*, 103 F.4th 732,742(9th Cir. 2024)(“Meta invites us to reconsider the limitations we have previously recognized and encourages us to adopt a broader rule that would effectively bar ‘all claims’ ‘stemming from their publication of information created by third parties.’”)

⁸¹ *Backpage.com's Knowing Facilitation of Online Sex Trafficking: Hearing Before the Subcomm. on Investigations*, 115th Cong. (2017); Statement of Frances Haugan, U.S. Senate Commission on Commerce, Science, and Transportation, Subcommittee of Consumer Protection, Safety and Privacy Sub-Committee on Consumer Protection, Product Safety, and Data Security (Oct. 1, 2021).

V. Principles to Consider in Reform

After nearly three decades of judicial distortion of §230 of the Communications Decency Act, the results have been clear:

The result is a § 230 that immunizes platforms from the consequences of their own conduct and permits platforms to ignore the **ordinary obligation that most businesses have** to take reasonable steps to prevent their services from causing devastating harm. But this conception of § 230 immunity departs from the best ordinary meaning of the text and ignores the context of congressional action.⁸²

Therefore, Congress must act.

Such a revision should be multi-tiered to reflect this complex terrain, but not be overly unwieldy to delay enactment. Two principles the Conference Committee identified in 1996 remain relevant in today's reality: (1) companies should have protection from suit when they remove harmful content from platforms, and (2) companies should face the same liability as all other industries when they facilitate harm or create harmful products. In recent years, Congressional Committees have explored a variety of approaches. In constructing a multi-tiered revision, some promising components of reform may include, but are not limited to, aspects of the following.

First, the law should retain Good Samaritan immunity of §230(c)(2). As originally intended, an ICS should receive immunity from liability for good faith removal of material it "considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."⁸³ Second, Congress should eliminate the §230(c)(1) shield while retaining Good Samaritan protection of § 230(c)(2). Any immunity beyond that for Good Samaritan removal has been distorted by tech companies and simply does not serve any of the legislation's purposes. It neither assists in limiting exploitive and indecent content, nor does it advance the development of the internet – an industry not in need of special consideration. With neither the purpose of the CDA nor Telecommunications Acts advanced, § 230(c)(1) immunity constitutes a failed experiment.

Additionally, it is important to note that this is simply a removal of immunity from suit, not a finding of liability. This simply allows those who allege a platform harmed them to have their day in court. Plaintiffs or prosecutors would still need to prove their case. But plaintiffs would be able to obtain discovery, and platforms would no longer enjoy secretive business practices they should know are

⁸² Anderson v. TikTok, Inc., 116 F.4th 180, 191 (3d Cir. 2024) (Matey, J. concurring in part and dissenting in part)(emphasis added).

⁸³ 47 U.S.C. § 230(c)(2).

harmful and only discoverable by congressional investigations or whistleblowers. Rather, platforms will have to assess risk in business decisions similar to every other business.

The claim that this will lead to crippling litigation is unfounded. Analogously, copyright law affords such holders rights to prevent infringement online and this is carved out of §230 protections.⁸⁴ The jurisprudence in this analogous space has developed, and here companies have implemented clear notification and takedown procedures. Parties now know what a reasonable effort is to remove copyrighted material, and although § 230 does not give platforms immunity with copyrighted works, the internet still thrives. Similarly, in this area of the law affecting victims, the jurisprudence which has not been allowed to develop under a regime of de facto near absolute immunity will emerge, a reasonable duty of care will become clear, and the risks a business takes will be influenced by potential liability similar to all other industries.

Third, the internet is no longer a nascent endeavor but a massive, thriving, and self-sufficient ecosystem. As Justice Kagan raised during a recent oral argument, “every other industry has to internalize the costs of its conduct. Why is it that the tech industry gets a pass?”⁸⁵ Platforms, therefore, should be liable for facilitating, hosting, amplifying, or distributing materials that they should know are illegal or exploitive (including but perhaps not limited to CSAM, sexualized images of children, human trafficking, nonconsensual pornography, and deepfake sexualized imagery). The concept of the original § 230—that a website should not be liable as a publisher—originated because a publisher can be aware of the illegality of the content. Platforms today, unlike in 1996, collect a massive amount of data. These companies have demonstrated they are capable of leveraging vast amounts of customer data for profit and should also be required to use that data to ensure protection.⁸⁶

Fourth, most industries are expected to exercise reasonable care in their design and function. There is no reason why this industry, which is so far reaching, should be exempt from such a requirement. By having such a standard similar to other businesses, platforms would be allowed a defense that they complied with a reasonable standard of care. This use of best practices should be a trial defense, not a source of immunity from suit. In that context, aggrieved persons would have their day in court to learn the information possessed and actions taken by the platforms who, in turn, would have an opportunity to

⁸⁴ § 230(e)(2); See, Dan Solove, [Restoring the CDA Section 230 to What It Actually Says](#), **TeachPrivacy** (Feb. 4, 2021) (noting that while a platform is not required to remove an unconsented to nude photo, it is required to do so if the image is copyrighted).

⁸⁵ *Gonzales v. Google*, 598 US 617 (2023).

⁸⁶ Congress may also want to consider clarifying the mens rea of 47 U.S.C. §230(e)(5)(A) which tech has succeeded in obfuscating contrary to the intent of the amendment.

rebut the allegation by demonstrating their actions taken to prevent such harm fit within the standard of care for its particular business.

Fifth, states should be allowed to enforce their criminal laws. For several years, the National Association of Attorneys General has called upon Congress to amend § 230(e)(1) to state that “[n]othing in this section shall be construed to impair . . . any other Federal or State criminal statute.”⁸⁷ The ability of states to enforce their own criminal laws against platforms who harm their citizens is essential. For example, currently, states’ hands are tied when their citizens’ images are distributed online by platforms in violation of state criminal laws. To preclude the ability of states to enforce criminal laws that mirror federal laws is unnecessary and harmful to victims.

Conclusion

There are many possible actions Congress can take to address online exploitation. However, the ecosystem that creates the ability to harm with such impunity stems from the distortion of §230 of the Communications Decency Act. Rather than solely draft legislation that reacts to harms occurring, the goal should be to create a safer digital space preventing such harms in the first place. This will not take place until the industry that houses the material and facilitates the harm faces accountability for their actions similar to almost every other industry.

⁸⁷ Letter from Nat’l Ass’n of Att’ys Gen. to Sen. Rockefeller, Sen. Thune, Rep. Upton, and Rep. Waxman (July 23, 2013), <https://www.eff.org/files/cda-ag-letter.pdf>; NAAG Supports Amendment to the Communications Decency Act, Nat’l Ass’n of Att’ys Gen. (May 23, 2019), <https://www.naag.org/press-releases/naag-supports-amendment-to-the-communications-decency-act/> [<https://perma.cc/B8HZ-S4F3>] (noting support for a letter signed by forty-seven attorneys general to amend § 230 to allow the enforcement of state law).

RESPONSES OF PROF. MARY GRAW LEARY TO QUESTIONS
SUBMITTED BY SENATOR ALEX PADILLA

Questions For the Record

*Mary Graw Leary,
Professor of Law, The Catholic University of America*

**Children's Safety in the Digital Era: Strengthening Protections and
Addressing Legal Gaps**

Senate Judiciary Committee
March, 2025

Introduction

Thank you for the additional question regarding character-based AI chatbot apps. While this technology is not a specific area of my expertise, it does illustrate some of the several problems of the toxic combination of (a) an unregulated tech industry, (b) that releases dangerous untested products harmful to children; and (c) that possesses near de facto absolute immunity for the harm it causes by doing so. Phrased another way, the release of AI chatbot apps without adequate safety measures in place is a product of this unregulated environment and an outdated § 230 of the Communications Decency Act. That Act not only fails Congressional goals of incentivizing a safer internet, but encourages the opposite, which is especially dangerous with ever evolving technologies such as these. This situation further illustrates that Congress cannot meet 21st Century problems with a 20th Century tool. This QFR answer will address the harms being caused children through unregulated AI chatbot apps, the basic need for legislative action, the role of § 230 in this discussion, and potential steps to consider.

1. Children Suffer When Unsafe Products Are Unleashed on Them

First, there have been documented cases of how these products inflict harm on children. These character based chatbot apps are designed to replicate conversations with an actual person – using AI to adapt to the user and create their own content.¹ These chatbot apps are designed to appear enticing to young people, designed to encourage ongoing and continual use, and expose children to harmful content. Documented cases exist of such bots providing youth dangerous advice to engage in harmful behavior, sharing harmful content, and exposing children to sexualized imagery and conversation. Some examples include chatbots encouraging a child to kill his parents; encouraging a child to kill himself; providing dangerous guidance on topics including drug use, self-harm, eating disorders and sexual abuse; causing severe depression; and causing addictive dependence and isolation.² Because of their developing brains, children are at great risk of negative effects of such a product. Children are more vulnerable and less able to process the nuances of an artificial bot giving them this harmful information when designed to appear to be a human friend.³

¹ AI Chatbots and Companions – Risks to Children and Young People, https://www.esafety.gov.au/newsroom/blogs/ai-chatbots-and-companions-risks-to-children-and-young-people#:~:text=the%20United%20States,-_What%20are%20the%20risks%3F,to%20overuse%20and%20even%20dependency; Queenie Wong, *Teens Are Spilling Dark Thoughts to AI Chatbots. Who's To Blame When Something Goes Wrong?*, The Los Angeles Times (Feb 25, 2025); Bobby Allyn, *Lawsuit: A Chatbot Hinted a Kid Should Kill His Parents Over Screen Time Limits*, NPR (Dec. 10, 2024).

² AI Chatbots and Companions – Risks to Children and Young People, <https://www.esafety.gov.au/newsroom/blogs/ai-chatbots-and-companions-risks-to-children-and-young-people#:~:text=the%20United%20States.What%20are%20the%20risks%3F,to%20overuse%20and%20even%20dependency>.

³ See, e.g., Matthew Hastings, *What Do Parents Need to Know About AI Character Chatbots?*, Univ. of Col Newsroom (Dec. 2, 2024), <https://news.cuanschutz.edu/news-stories/what-do-parents-need-to-know-about-ai-character-chatbots>.

2. No Other Industry Can Release Such a Dangerous Inadequately Tested Product That Harms Children and Avoid Accountability for Doing So

This leads to the obvious question of how is it that an industry could put onto the market such a dangerous product without being confident that it is safe and, once it discovers the harm it causes, keep it on the market? The answer is found in two components of our technology ecosystem: the industry is entirely unregulated and the companies are not incentivized to make their products safe because of the current distorted interpretation of § 230 of the CDA.

Regarding regulation, I noted in my original testimony as well as the article entered into the record that there is a natural historical arc of regulation compellingly outlined by Professors Danielle Keats Citron and Benjamin Wittes in their 2017 article, *The Internet Won't Break*. They point out that historically burgeoning industries can begin without regulation. However, when these industries mature, the government recognizes they reached a stage where the industry can cause broad harm by a small error, and the government takes on its required role of public protector and provides minimal safety guardrails to fulfill that obligation.⁴ Examples of this historical arc include public transportation, utilities, motor vehicles, water supply, chemical manufacturing, food supply, and agriculture. When these industries grew to where they could cause serious harm to large numbers of people, some form of outside oversight occurred.⁵

However, in the context of these digital platforms, the government has not intervened in that traditional way. The result is unprecedented harm as has been outlined in many congressional hearings.

This is where the role of §230 of the Communications Decency Act is particularly insidious. Although intended to be a shield for platforms' efforts to protect children, tech companies have distorted it to provide a near absolute de facto immunity for actions that harm children and other users. Consequently, in addition to having the luxury of an unprecedented unregulated climate, § 230 provides businesses an additional incentive to release unsafe products to the market: protection from any liability for doing so. Consequently, these companies and their surrogates not only vigorously oppose common sense regulation but also seek wider immunity.⁶

Although the scope and size of the tech industry alone compel regulation and Congressional action, the nature of the industry also compels greater Congressional oversight. The rapid expansion of AI is breathtaking, in just two years society has been transformed and there are currently hundreds of chatbot companion apps, millions of characters, and some

⁴ Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 Fordham L. Rev. 401, 406 (2017)..

⁵ *Id.*

⁶ In 2024 tech companies continued to attempt to expand their already de facto near absolute immunity. *Calise v. eta*, 103 F.4th 732,742(9th Cir. 2024)(“Meta invites us to reconsider the limitations we have previously recognized and encourages us to adopt a broader rule that would effectively bar ‘all claims’ ‘stemming from their publication of information created by third parties.’”)

companies reaching a \$1 billion valuation in that time.⁷ While traditionally courts can provide some relief to those harmed by dangerous products, they are hampered in doing so when the product is part of the tech industry. The judicial system is both reactive and slow moving and not effective when the product is related to these technologies and is rapidly changing. Therefore, relying on courts to somehow mitigate these harms is particularly inappropriate in a rapidly changing sector. Legislation is necessary.

3. §230 Has Not Only Helped Create This Problem, It Amplifies It

The above section describes how § 230 of the CDA helps cause the problem of character chat bot apps – or other dangerous products – being unleashed on the public generally, and children in particular, by providing an incentive to do so with impunity. This section describes how § 230 then is being utilized to preclude access to justice by perverting it even more than has already occurred.

Textually, § 230 of the CDA *should* provide no protection for generative AI platforms, because the content is generated by the platform and § 230 of the CDA specifically protects platforms only when the content is from a third party. Specifically, § 230 of the CDA provides protection for “interactive computer services” (ICS) not “information content providers” (ICP).⁸ An “information content provider” includes “any person or entity that is responsible, in whole *or in part*, for the *creation or development of information* provided through the Internet or any other interactive computer service.”⁹ By creating the character and generating the content of the communication between the user and character, the bot is creating the content. Furthermore, courts have recognized that ICS’s can also be information content providers and lose protection.¹⁰ Therefore, AI generated content should not be protected at all by § 230 because it is content generated in whole or in part by the platform which is then acting as an information content provider.

But Congress should take no comfort in such textual clarity, as the current state of the distorted § 230 of the CDA has been and will continue to be utilized by said platforms to argue they are not responsible for the harms their AI causes.¹¹ Indeed they have used the “material contribution” test to argue that although they assist in the content development, they are not content providers. Amazingly, the blame for the content then goes back on the user.¹²

⁷ Queenie Wong, *Teens Are Spilling Dark Thoughts to AI Chatbots. Who’s To Blame When Something Goes Wrong?*, The Los Angeles Times (Feb 25, 2025).

⁸ 47 U.S.C. §230(c).

⁹ 47 U.S.C. 230(f)(3).

¹⁰ *E.g., Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1163 (9th Cir. 2008).

¹¹ Justice Thomas has noted the hypocrisy of the tech industry’s claim of s230 protection for their own content. “In the platforms’ world, they are fully responsible for their websites when it results in constitutional protections, but the moment that responsibility could lead to liability, they can disclaim any obligations and enjoy greater protections from suit than nearly any other industry.” *Doe v. Snap, Inc.*, 144 S. Ct. 2493, 2494 (2024) (Thomas, J., dissenting denial of certiorari) (mem.).

¹² *Compare, Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1163 (9th Cir. 2008) (finding the platform materially contributed to the illegality by providing a drop down menu of terms) with

Consequently, the textual clarity of § 230 is not helpful to the question of whether §230 should be updated to remove this protection. It absolutely should.

Many courts have articulated the need for § 230 of the CDA to reflect the current technological realities, not the outdated ones of the 1996 dial up internet era. Just last year, a Ninth Circuit judge warned of AI when noting that the application of §230 of the CDA to technologies unimagined in 1996

stretch the statute’s plain meaning beyond recognition. And they will continue to occur unless we consider a more limited interpretation of § 230(c)(1)’s scope of immunity. *In a world ever evolving and with artificial intelligence raising the specter of lawless and limitless protections under § 230(c)(1),* we should revisit our precedent and ensure we have grounded its application.¹³

Similarly, Justice Thomas articulated that states and the federal government must be free to update their laws “to make them more appropriate for an Internet-driven society.”¹⁴ This notion of a changing and more protective legal regime as technologies rapidly develop has been articulated by scholars¹⁵ and even during the debate of the original CDA.¹⁶

4. Potential Responses to the Emergence of AI Chatbots

Therefore, the answer to these challenges is a more regulated internet and an end to §230’s incentive to release harmful products with impunity. More specifically, there are two components to a Congressional response to the problem of AI chatbots in an unregulated industry with a current legislative regime of incentivizing harmful product release. The first is eliminating that incentive by reforming § 230. The second is implementing regulatory legislation that is responsive to AI and other technologies.

Regarding § 230, as my original testimony addresses, Congress should remove § 230(c)(1) of the CDA entirely. Providing any sort of protection to platforms for harmful products for children flies in the face of the original intent of § 230 of the CDA. If § 230(c)(1) of the CDA ever did serve a purpose, the internet is no longer a nascent industry in need of any protection. Rather, the people need protection from an unregulated industry which causes harm on them.

Within such a reform, Congress should also consider specifically including language in § 230 that AI generated content is not protected in any form by § 230 of the CDA.¹⁷ This would preemptively address some of the claims in courts that AI is protected by § 230 of the CDA. In

O’Kroy v. Fastcase, Inc., 831 F.3d 352 (6th Cir. 2016)(finding search engine did not materially contribute to how information was displayed although it engaged in some form of editing information).

¹³ *Calise v. Meta Platforms, Inc.*, 103 F.4th 732, 747–48 (9th Cir. 2024) (Nelson, J., concurring)(emphasis added).

¹⁴ *Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC*, 141 S. Ct.13 (2020)(mem.).

¹⁵ Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 Fordham L. Rev. 401, 406 (2017).

¹⁶ 142 **Cong. Rec.** S686 (daily ed. Feb. 1, 1996) (statement of Sen. Pressler) (“I predict that this will be succeeded someday as we get into the wireless age by another act, maybe in 10 or 15 years. But this Telecommunications Act will provide us with a road map into the wireless age and into the next century.”).

¹⁷ See, e.g., A Bill to Waive Immunity Under Section 230 of the Communications Decency Act of 1934 [sic] for Claims and Charges Related to Generative Artificial Intelligence, S. 1993, 118th cong. (2023-2024).

courts addressing this problem, a very fact specific inquiry occurs regarding how the particular AI product functions and distinctions between AI operations can be made which will cause great disparity and confusion among the courts.. In order to prevent splintered court decisions, Congress can act now to answer the question of whether AI chat bots are considered content creation with an emphatic yes.

Such a reform is essential because of the nature of the technology. Currently, if § 230 of the CDA protects a platform for harm caused by third party content, the argument goes that the victim can still seek liability from the content creator. However, with AI, there is no other individual content creator and a victim will literally be left without any recourse.¹⁸ Such is not acceptable.

Reform of § 230 of the CDA is only a minimal step. It simply allows injured parties access to a courtroom to attempt to prove their case. Such a reactive approach, while providing some deterrence, does little to prevent the harm in the first place.

Secondly, the tech industry in general, and the AI chatbots in particular, should face guidelines exposing their hosts and developers to penalties if unsafe. As is expressed in recent legal claims against Character AI, a fundamental problem is the industry releasing untested or inadequately tested chatbots to the public which are deeply flawed and dangerous to consumers.¹⁹ Beyond § 230 of the CDA, the products raise issues about product design having nothing to do with publication. Here, previously proposed legislation requiring such platforms to exercise the same duty of care as other industries, seems an essential component of safety. Elements of this approach are found in the Kids Online Safety Act and present a promising step to such platforms being held accountable for the release of dangerous products.²⁰ Safety by design must be embedded within the industry as well. That being said, a duty of care and requirement of safety by design should be accompanied by the repeal of at least §230(c)(1) protections. This portion of § 230 of the CDA has proven to incentivize the production of harmful products and serves no purpose.

Within these guidelines, Congress should include elements of transparency and auditing. It is essential that the technology behind the AI and algorithms be transparent. Furthermore, efforts of the platforms to test them prior to deployment should be an essential component of necessary acts prior to release. The results of these audits should be available for review.

Third, Congress should consider a regulatory body to oversee this industry. This body should remain under the control of Congress. Such an office could provide, *inter alia*, standards of care and best practices, which would give the industry a sense of acceptable safety standards.

As Congress considers the future of the internet and the valid concerns of the government's ability to stay in pace with rapidly changing technologies, there is an additional model to which some nations are turning due to the need for a rapid response to quickly developing threats. This

¹⁸ See, Jake Gray and Abbey Block, *Beyond the Search Bar: Generative AI's Section 230 Tightrope*, Business Law Today (Nov.2024).

¹⁹ *Garcia v. Character Techs, Inc.*, No.6:24-CV-01903 (M.D. Fla. Oct. 22, 2024).

²⁰ Kids Online Safety Act, S. 1409, 118th Cong. (2023).

model is the creation of an E-Safety Commissioner. Australia was the first nation to do so. The purpose of the office is “to help safeguard [the public] at risk of online harms and to promote safer, more positive online experiences” and the Commissioner takes measures aimed at “preventing online risks, reducing the impacts of harms, and building safer digital spaces.”²¹ Created in 2015, when Australia streamlined its online safety legislation in 2021 in the Online Safety Act, the Commission’s mission included prevention, protection, and proactive system change.²²

Essential to that effort was the 2021 Online Safety Act leading to a list of Basic Online Safety Expectations (BOSE) the government required of platforms.²³ These provisions, enforceable with significant civil penalties, outline Congress’s expectations that social media, platforms, and other providers in the tech industry, will take reasonable steps to incorporate safety by design for all users.

By creating such **Congressional** expectations and then establishing an E-Safety Commissioner, Congress could embark on a more proactive regime necessary for the today’s evolving digital world. Such an office likely would more nimbly address emerging threats online than Congressional action could do. If its powers were drafted narrowly enough to respond to such threats with Congressional oversight, this office may prove to be a valuable tool to enhance online safety.

To be clear, reform of § 230 and the creation of a clear duty of care should not wait for the establishment of this office. The harms people are experiencing are immediate and significant; and Internet regulation and § 230 of the CDA reform are long overdue. That being said, Congress should think more systematically about how the federal government can be positioned to respond to future threats and not wait for the threats to emerge. Therefore, an E-Safety Commission is worth further consideration.

Conclusion

AI Chatbots pose a serious threat to users, especially youth. No other industry could release a dangerous product to children with impunity. Court response to this will be slow and likely distorted. Therefore, Congress must act and do so in a way that is proactive and systemic. This has at least two major components to combat the uniquely toxic ecosystem that has been created by the distortion of § 230 of the CDA and a lack of meaningful regulation for such a powerful industry. At a minimum the §230 of the CDA reforms should include the removal of § 230(c)(1) protection, and an explicit statement that those who develop, finance, host and power AI technologies are responsible for the harm their products create. Finally, meaningful regulation which lays out Congressional expectations of the tech industry and penalties for failure to conform are essential and the possible creation of an e-safety commissioner with Congressional oversight has promise to execute these visions.

²¹ <https://www.esafety.gov.au/about-us/what-we-do>

²² <https://www.esafety.gov.au/about-us/what-we-do>

²³ Online Basic Online Safety Expectations - Determinations 2022, <https://www.legislation.gov.au/F2022L00062/latest/downloads>

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

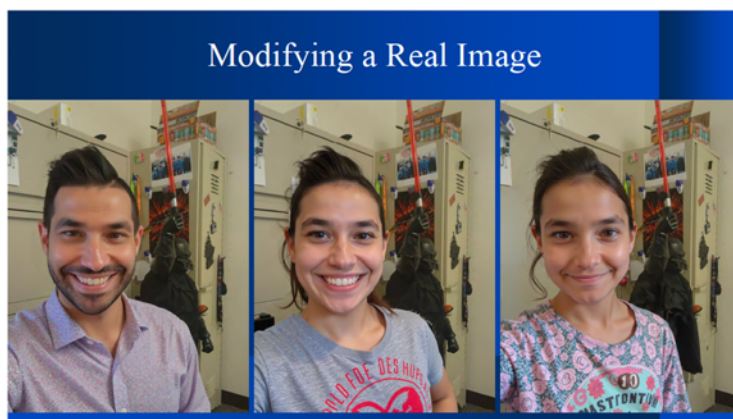
for the

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 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 States¹

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 words 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.

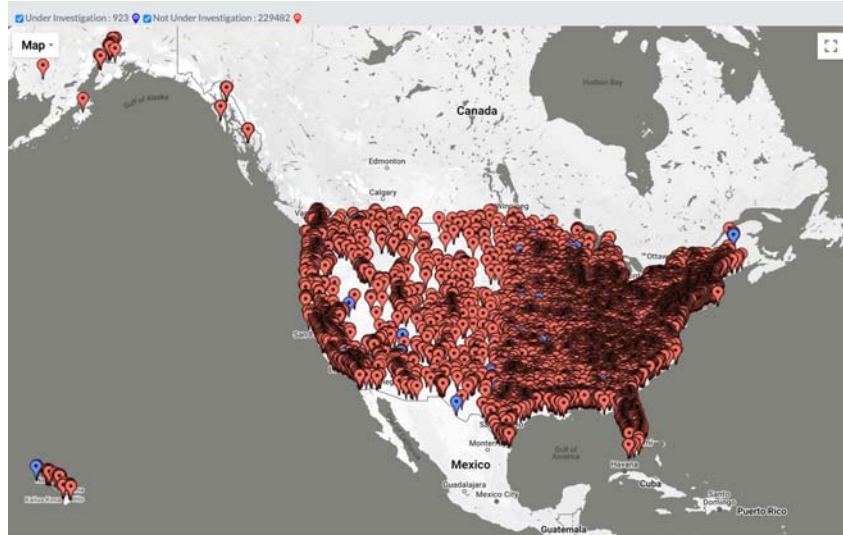
Most of the investigative leads provided by service providers, through NCMEC, to the ICAC Task Forces are not actionable, meaning they do not contain sufficient information to permit an investigation to begin. The lack of uniformity in what is reported by service providers results in law enforcement 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

SUBJECT / STARTED BY		REPLIES / VIEWS	LAST POST
	Guidelines and Staying Safe  Started by Glover	9 Replies 58,859 Views	06 July, 2022, 10:37:54 by thewhitewings
	Pedomom: Thinking about my daughter having sex arouses me totally  Started by anonone • 1 2 3 •	38 Replies 40,261 Views	Today at 17:29:39 by Sharon
	Underage Kids and Orgasms  Started by danteovergl • 1 2 3 •	30 Replies 23,944 Views	Today at 07:10:02 by littleboylost
	confused mom  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?  Started by Pedomom • 1 2 3 •	30 Replies 20,552 Views	07 May, 2022, 19:44:54 by RogerTheStrangler
	Masturbating around children  Started by Enchantress • 1 2 3 •	37 Replies 22,129 Views	25 April, 2022, 17:00:08 by ampmaven
	How to stop with those less than legal age?  Started by Robertboy	5 Replies 1,378 Views	24 April, 2022, 03:42:03 by LGSlove127
	new kids  Started by gblvr	11 Replies 3,081 Views	23 April, 2022, 13:06:08 by SecondChance
	Baby sitting a friend's 9 year old daughter twice a week  Started by Exiler • 1 2 •	29 Replies 11,972 Views	20 April, 2022, 22:05:16 by LGSlove127
	Thoughts on oral sex with kids 0-2?  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.

Questions for the Record from Senator Alex Padilla
Senate Judiciary Committee
“Children’s Safety in the Digital Era: Strengthening Protections and Addressing Legal Gaps”
February 19, 2025

Questions for John Pizzuro

1. Children today interact with a relatively new consumer product, character-based AI chatbot apps. Many of these services have been flooded with age-inappropriate chatbots—which may expose young users to sexual or suggestive AI-generated imagery or conversations. Further, conversations with these chatbots can end tragically—since 2023, at least two individuals have died by suicide following extensive conversations with AI chatbots. How would you recommend this Committee think through and respond to the risks posed by this emerging consumer product category, given your experience with child online safety?

AI Chatbots is increasing at an alarming rate. The lack of regulations makes it challenging. Even if the AI Chatbot originally conforms to an Apple or Google App Store the updates do not get tested therefore exposing risk. As an example, even Chat GPT will tell you how to exploit children if asked in the proper way. There are a couple of solutions one is that we are working on Bill Text (We have a rough draft – The Raven Act) which would provide a solution that would be tenable for all parties. It is device based, age/identity identification which would protect children and seniors. Rather than go through multiple apps it would require just one permission for the device that could be turned by the account owner. This could override apps in which a child for example is underage or even prevent children from accessing an AI Chatbot. What makes this solution plausible is that it doesn't impact privacy since the device knows how old you are, it puts the discretion to the parent or account owner allowing for them to determine what is appropriate and not appropriate. All the app stores would have to require is “a Handshake” between an app and a device. It is also not feasible to require every app manufacturer to comply since there are so many apps.

A second solution would be the creation of a third-party program that can ensure that an app meets an AI safety standard.

A P P E N D I X

The following submissions are available at:

<https://www.govinfo.gov/content/pkg/CHRG-119shrg61324/pdf/CHRG-119shrg61324-add1.pdf>

Submitted by Chairman Grassley:

Adoptive mother of CSAM victims-survivors, February 16, 2025, letter—Redacted	2
Alliance to Counter Crime Online, November 25, 2024, letter	4
Amy, plaintiff in a CSAM class-action lawsuit, February 17, 2025, letter	7
Barnett, Elizabeth, parent of CSAM victim, February 23, 2025, letter	8
Chelsea, CSAM victim-survivor, February 17, 2025, letter	11
Doe, Jane, adoptive mother of CSAM victims-survivors, February 16, 2025, letter	13
Emily, CSAM victim-survivor, February 16, 2025, letter	15
Sexual Exploitation and Abuse of Children Coalition and End OSEAC Survivors' Council, statement	17
Erika, CSAM victim-survivor, February 17, 2025, letter	20
Gabriel, CSAM victim-survivor, February 14, 2025, letter	22
Haba, Lisa D., et al., February 17, 2025, letter	25
Henley, CSAM victim-survivor, February 16, 2025, letter	30
Kauzie, CSAM victim-survivor, February 16, 2025, letter	32
Leary, Mary Graw, <i>Villanova Law Review</i> , Volume 70, 2025, article	34
Mother (I) of a CSAM victim-survivor, February 16, 2025, letter—Redacted	97
Mother (II) of a CSAM victim-survivor, February 16, 2025, letter—Redacted	99
Mother of J, a CSAM victim-survivor, February 17, 2025, letter	101
Susanna, mother of CSAM victims-survivors, February 16, 2025, letter	102
Victim-survivor of CSAM, February 15, 2025, letter—Redacted	104
Victim-survivor of CSAM, February 16, 2025, letter—Redacted	105

